ISSN NO. (Print) : 2320-2106, (Online): 2321-2063

International Journal of Advance Computational Engineering and Networking(IJACEN)

Volume No. 12
Issue No. 1
January - April 2024

ENRICHED PUBLICATIONS PVT. LTD

S-9, IInd FLOOR, MLU POCKET,
MANISH ABHINAV PLAZA-II, ABOVE FEDERAL BANK,
PLOT NO-5, SECTOR-5, DWARKA, NEW DELHI, INDIA-110075,
PHONE: - + (91)-(11)-47026006

ISSN NO. (Print) : 2320-2106, (Online): 2321-2063

International Journal of Advance Computational Engineering and Networking(IJACEN)

Aim & Scope

“International Journal of Advance Computational Engineering and Networking(IJACEN)”(ISSN NO. (Print) : 2320-2106, (Online): 2321-2063) a peer-reviewed and free open access journal aim to provide the complete and a reliable source of information on current developments in the fields of Computer Science, Information Technology, Software Technology, Networking and Communication. The emphasis will be on publishing quality articles rapidly and openly available to researchers worldwide.

Manuscripts submitted to “International Journal of Advance Computational Engineering and Networking(IJACEN)” must be prepared in English and are subject to a rigorous and fair peer-review process. All submitted papers must be original work that has not been published or under consideration for publication elsewhere. Manuscripts should be typed double space on A4 size paper using font size 12 and preferably not more than 8 pages in length inclusive of tables, figures and illustrations.

All submissions will be peer-reviewed. The scope of “International Journal of Advance Computational Engineering and Networking(IJACEN)” covers all aspects Computer Science, Information Technology, Software Technology, Networking and Communication etc.

“International Journal of Advance Computational Engineering and Networking(IJACEN)” is a Monthly journal(12issues/year). Papers solicited for “International Journal of Advance Computational Engineering and Networking(IJACEN)can be in the form of survey/tutorial, regular papers, brief papers, case studied and technical correspondence. The journal provides a national and international forum for rapid publication of work describing theoretical as well as practical aspects.

At IJACEN we publish peer-reviewed scholarly journals indexed with most international A&I databases. Most of these journals provide immediate free access to the full text of articles in HTML format. Authors can also archive the journals themselves. The majority of the journals do not charge for article submission, processing or publication. Our open-access policy increases the visibility and accessibility of the published content. To find the access, archiving and copyright policy for a particular journal please use the search facility above.

ISSN NO. (Print) : 2320-2106, (Online): 2321-2063

EDITORIAL BOARD

Dr. P. Suresh
Professor, Karpagam College of Engineering,Coimbatore
Tamilnadu, Email:ijacenitr@yahoo.com

Dr. John Dayton, Program In English, Rochester Institute of Technology, UAE	**Dr. Ihsan Mohammed Abud,** Department of Physiology, University of Kufa, Iraq

Publication and Distribution Head

Prof. Vinod Tyagi
Institute of Research and Journals, India
Email: editor@iraj.in

Reviewers

S. Purushothaman Scientist, ISRO Satellite Centre, ISRO Dept. of Space, Govt. of India	**Er. Rajashekar M. Hiremath** Assistant manager(operations) Jindal steel and power Ltd. Pellet plant(4.5MTPA) Barbil Orissa
Dr. Sakkaravarthi Ramanathan Co-Director of R&D and Professor, Computer Science Department, EGS Pillay Engineering College, Nagapattinam, Tamil Nadu, India	**Prof. ANAND NAYYAR** Assistant Professor, Department of Computer Applications & IT, KCL Institute of Management and Technology
Dr. Rawan Abulail Professor, Dept. of CS & IT, Philadelphia University Dr. Yuchou Chang University of Wisconsin, United States	**Dr. Krishnan A** K.S.R College of Engineering, India
Dr. Duraiswamy K K.S. Rangaswamy College of Technology, India	**Dr. Wathiq Mansoor** American University in Dubai, United Arab Emirates
Dr. Abdel-Hamid Mourad United Arab Emirates University	**Dr. Ivan Bruha** McMaster University, Canada
Dr. Viliam Makis University of Toronto, Canada	**Dr. Ramesh Agarwal** Washington University in St. Louis, United States Dr. Peter Milligan Queen's University Belfast, United Kingdom
Dr. Periasamy P.S K.S.R College of Engineering, India	**Mr. Gnanajeyaraman Rajaram** PVPCETW, India
Dr. Bommanna Kanagaraj PSNA College of Engineering and Technology, India	**Dr. Sasikumar S** Jayaram College of Engineering and Technology, India

ISSN NO. (Print) : 2320-2106, (Online): 2321-2063

International Journal of Advance Computational Engineering and Networking(IJACEN)

(Volume No. 12, Issue No. 1, January - April 2024)

Contents

ISSN NO. (Print) : 2320-2106, (Online): 2321-2063

Survey on Multimedia Security and Visual Cryptography

[1]Abhilash S Nath, [2] A. Jeyasekar

[1]Research Scholar, Dept. of Computer Science and Engg, SRMIST,KattankulathurCampus, Chennai 603203

[2]Associate Professor, Dept. of Computer Science and Engg, SRMIST, Kattankulathur Campus, Chennai 603203

E-mail: [1]abhilass@srmist.edu.in, [2]jeyaseka@srmist.edu.in

ABSTRACT

The people using internet has become so extensive across different sectors in day to day life. Security is the important feature different across the platform and mobile applications we use. The important aspect in the sectors is usage of the data having significant role in identifying the user preferences in using the data for video, text and games etc. Due to the large volume of data consumed by the customers is high it"s difficult for user to identify the identification of the pattern of data that is stored by the remote servers .The advertisements and the thumbnails that come across as your search relates can be seen. This understanding by the service providers or the sites that we visit store our preferences in choosing the content matters .Mostly people chooses the video content for news, entertainment .The people also uses camera for home security and even for live streaming personal mobile cameras used. These all uses huge amount of data. The information loss during the communication between the devices through internet there is a lack of features which even cannot be controlled by the protection software"s. To avoid all leaky information from the transfer of data technique called visual cryptography is used. In this survey, present an overview of the characteristics, security threats and major security challenges. The contribution of the survey will lead to understand the visual cryptography and security facets of it. The various techniques existing in the visual cryptography will help to figure out the improvement of cryptographic technique in various years. Some identified areas of security which can also affect our day to day life which give motive to find new ways of security mechanism.

Keywords - Internet, Visual Cryptography, Information Loss

I. INTRODUCTION

The network is collection of interconnected devices. The network has been secured for large number of devices .There are different type of attacks which is happening in computer networks. The activity of hackers in to gain huge amount of information in multimedia data would generate a major concern for security. The multimedia applications created by the users find more vulnerable to different attacks. The major part of the idea is encryption of the large number of image shares. These attacks used efficient and secure way to break in to a system. While understanding the side channel attack by leaking information, the attacker can infer the activities based on size of the data of an encrypted video stream. The video market is expected to reach dollar 45 billion by 2020. Saving the bandwidth and space for storage a encoder removes spatial redundancy .Difference coding causes significant side-channel information leakage. Some of activities increase the storage space and increase the size of the traffic data. The visual cryptography increases the safety of the image in a huge way it help to store in a very important way it decreases the storage space of the data and increases the transmission of the data in a huge manner. Big Organizations wants strong security devices for analyzing the vulnerabilities in their networks. But with big scale networks and managing their complex configurations technically difficult.

The network has to be changed with configuration change in other networks. The network admin wants to respond newly invented weakness by giving new patches and changes to the network configuration or utilizing resources to reduce the risk from attacks. Side-channel attacks gain technical information in the form power differential analysis and black-box attacks. The cases in the side-channel include cache attack, timing attack, power-monitoring attack and differential attack analysis.

II. TYPE OF SECURITY ATTACKS

In security attacks there are two type of attacks which are passive and active attacks. Passive attack means it make use of information without any need of algorithm. They learn the information but don‟t change the device operations. The main feature of passive attack is to monitor the operations. It just wants the information which is transferred. Release of message content and analysis of traffic which are types in passive attacks. Sensitive information collected through mail or talking through communication devices. The information received through email can identify by observing the pattern in which the length of messages and location of receiver or sender even though a message is encrypted. These types of attack are very difficult to track. But in active attack they change the operation of system .In the active attack there is alteration of the data by generating false data into the data stream. The active attack is divided into four types masquerade, modification, replay and denial of service.

In masquerade attack it pretends to be a person who is an attacker trying to send a message to the receiver which thinks its from original source or sender. This is done by capturing the privileges own by sender for obtaining more privileges by masquerading it has the same privileges. The modification of the information is altered. This is delayed to generate wrong exchange of message. The attacker will change a small part of the information during this delay and send to the receiver. In the replay attack the capture of message from sender to receiver where later replay message to receiver side.denial of service where it will prevent from communication services. This is denial of a service in a network. They are done for performance degrading. This can be targeted to any of the services this can be mostly seen when offers are made by particular website selling during festive seasons or launching of product for flash sales.

The passive attacks which are difficult to trace in the ways it procure the essential data from large network. The information which is transmitted through the network is large. The attacker can analyze different information by the pattern of the information passed across the network. Side-channel attack is a passive attack where information is gathered from system without algorithm which is implemented in the system itself.

A timing attack watches the movement of the data in and out of data of the CPU or memory on the hardware running the cryptosystem or algorithm simply by observing variations in how it takes to perform cryptographic operations. It might be possible determine the secret key. Such attacks involve statically analysis of timing measurements and have been demonstrated across the networks. In order to increase the confidentiality and privacy of the image share an encryption algorithm is used. Digital knowledge can be understood in different ways. It can be text, video, audio etc.

Private video can be transmitted and can be used for storage purpose easily. But due to the growth of information age security and the issue in privacy is very important. An authorized can login to account for his private data which is very sensitive. The answer to above problem is by encrypting the video to protect from an unauthorized access. The traffic in network during video streaming which has a pattern develops a threat of privacy of user. The network have huge amount of traffic due to the amount of data people use is very huge. Variable bit rate encoding used for balancing the video bit rate same. Video segments, its content and quality levels help the attacker to eavesdrop the traffic within a span of 3 minutes with a accuracy of 90 percent.. The quality level of video segment for playback, the pattern that is emerged helps for identification of videos. These mechanisms are seen in DASH which targets segment size variation of Variable bit rate and a particular traffic pattern. the identification of video in the traffic during video streaming without any change to video client and server. The differential bitrate based feature extraction for generating stable video features. The video finger prints and stream features are concatenated together for derive video identity by designing a partial matching method. The privacy of PC is challenged nowadays. There are two type of attacks passive an active attacks. The passive attack happens by eavesdrop of traffic from network side without direct contact with the device. The side-channel information of an encrypted traffic is used to collect the information about communications. This can be used for studying hugely for understanding the video streaming and web browsing etc. The research is mainly conducted on web traffic for its problems. Webpage can be monitored by the other people who can gain the personal information of user. It can be video information or text information mostly people prefer for storing their information. So some webpages have to hide some information to get away from eavesdroppers. The side-channel attacks on encrypted data, mixed with the selective sections of web apps are becoming a threat for privacy of user data processed by applications which is highly confidential and sensitive. Side channel is cl assified into two different categories of profiled and non-profiled where in profile phase a testing device which allows featuring the physical leakage and making an exact leakage model and non-profiled where attack is against a same target device to do a secret key extraction. Non-profile side channel attack includes differential power analysis, correlation power analysis variance ratio. Profile side channel attacks have stochastic approach and template attacks. Existing side channel attacks use an ideal measure environment with a mechanism to trigger the source code to get access to the target device. However this is not applicable to all real time events. Side channel data leakage in network studied vastly for more than a decade in the reference of cryptographic protocols and encrypted voice over internet protocol. Side-channel attacks have been there during the era of smart cards. Big Organizations wants strong security devices for analyzing the vulnerabilities in their networks. But with big scale networks and managing their complex configurations technically difficult. The network has to be changed with configuration change in other networks. The network admin wants to respond newly invented weakness by giving new patches and changes to the network configuration or utilizing resources to reduce the risk from attacks. The basic knowledge of visual secret sharing made for sharing visual information in the network. While other normal encryption or decryption processes, Visual secret sharing scheme has the advantage of make use of human visual system to decrypt the secret images without any complex mathematical computations. In this scheme, the encrypted image is split into m random shares. Then joining at least k shares to recover the original image. There is lot of research done in binary, grey-scale or color images. Since we used color and grey-scale image for hiding an information similar techniques are also used to hide image related to grey and color scale images. Most of the methods view on focusing to hide the information. Other than hiding, there is a method in which can restore the real image after reversing the hidden data for applications related to medical field and also geostrategic terrain images. These images must be highly secure and safe while sending to a specific person. Some uses a encryption method for securing the secret image with conventional encryption methods. The security depends whether the key generation algorithm is able to withstand a cryptanalysis or methods used to crack the key in possible ways. The image which is made into different shares using visual cryptography techniques and encrypting with a key is more secure.

III. VISUAL CRYPTOGRAPHY

Visual cryptography which was introduced by Shamir, Naor in 1995 is the technique based on human visual system. In this technique the encrypted data which is done by dividing the shares is decrypted by human eye. The complex structure of mathematical algorithms is not required in encryption and decryption. The images shares are encrypted into different number of images. When the images are stacked together to match the sub pixels among the images. The implementation of this scheme is 2 shares. The shares uses exclusive xor operations .This scheme is extended into k out of n shares where less than k shares are needed .k<=n. Naor and Shamir used for only black and white images. After some years Verheaul and Tilborg developed a scheme for colored images. They use random shares to cover the secret images but the quality of images recovered is poor. When the cryptanalysis of the image shares are considered if attackers are able to gain all the shares only then recovering of original image share can be done.

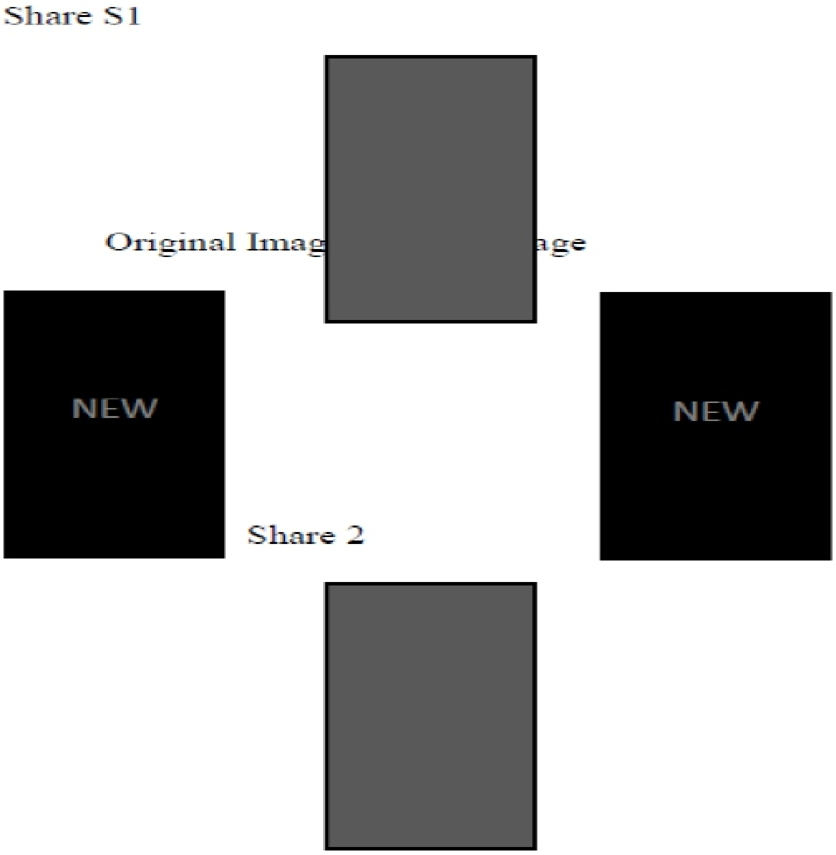


Fig.1: 2-out of 2 visual cryptography

In the above figure the representation of a secret image is made into shares in visual cryptography. The stacked image was obtained as a result of xoroperation .

Each pixel into a set of m black pixels white sub pixels in each of n shares for n-participants. When m=2 and n=2 its 2 out 2 scheme. To read all this images shares are stacked together. The result is reconstructed images of the secret image. But this image also contains noises. The display quality is affected by blackness and contrast value. Based on the degree of blackness there is deterministic model and probabilistic model. The (n,n)visual cryptographic schemes

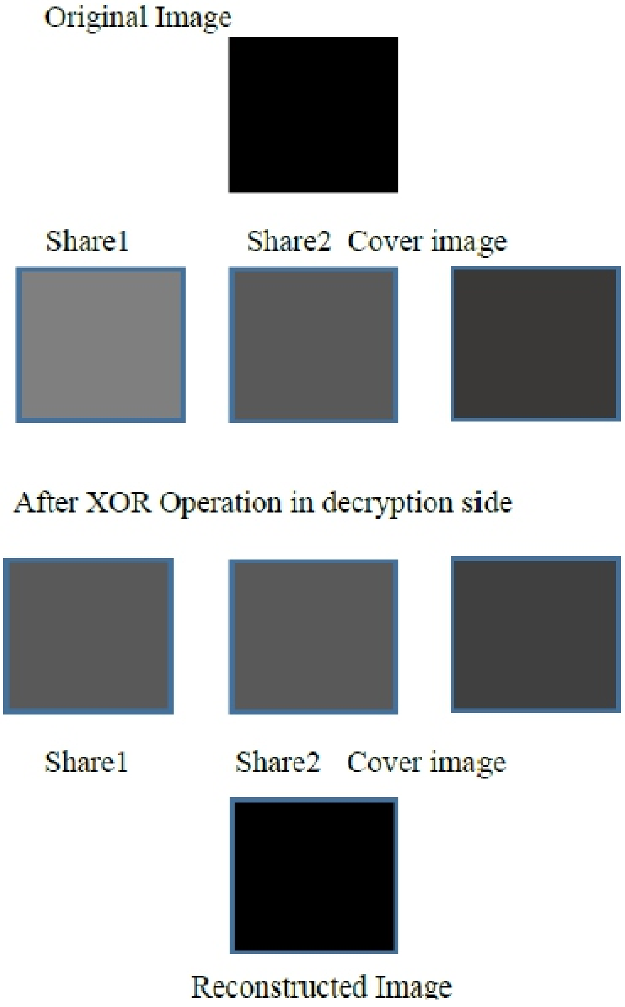
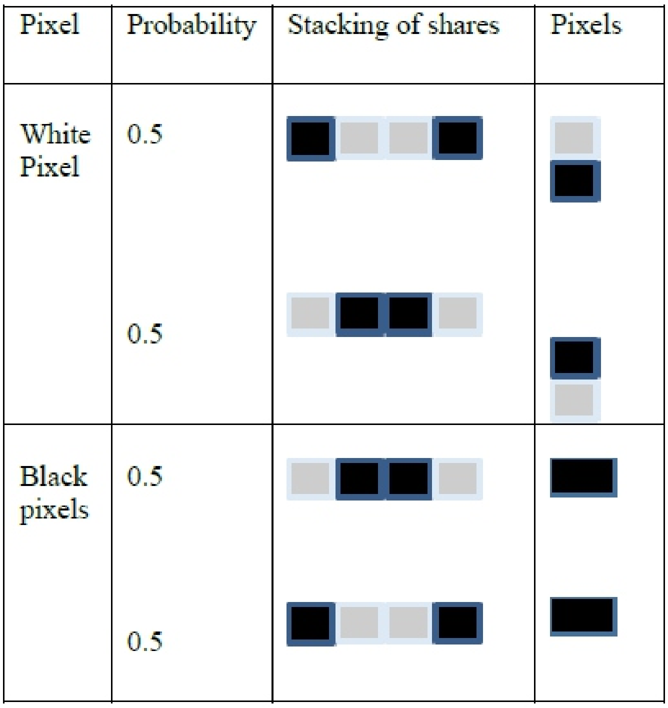


Fig.2 :k out of n visual cryptography

falls in first category and k,n visual cryptographic scheme in the later one. Researchers invented new visual cryptography techniques for gray scale and colored images. If The improvement of quality of images is limited in terms of development of VC algorithm where human eyes can perceive the image is not linked with the metrics used for quality measurement. There are researches where gray scale secret image is half toned by a quantizer of different level to generate binary images called halftone image and a threshold image. So different size invariant visual cryptography algorithms will be tested to the binary images these categories engulf the existing algorithms. In other category the intensity of block is quantized at various levels which turn represented by different patterns of binary images to accurate the local intensity. The secret images are encrypted into shares which can be considered as an analysis step for reconstructing the target image which is called synthesis step where image shares are binded .The target image in AbS process is pass on to analysis process where the pixel difference between target image and gray scale secret block is familiar to the encryption process.



Pixel	Probability	Stacking of shares	Pixels
White Pixel	0.5	■□□■	□ ■
	0.5	□■■□	■ □
Black pixels	0.5	□■■□	■■
	0.5	■□□■	■■

Fig.3: (2,2)scheme with 2 sub pixel stack

gray scale secret block is familiar to the encryption process. So the half toning method in encryption process can make changes to less the difference between the target image and secret block. i.e. the error between the original image and target image. Here in the above scheme m = 2 and n=2 so its called (2,2) scheme. The secret sharing expands the one pixel into several sub pixels. The recovered image is not the same exactly with the original one and makes it as noisy images.

When a pixel is black it choose two combinations. The two binded pixels become blacks. When binding white pixels in secret image are half-black and half white. The contrast of reconstructed image degraded by half percentage because degradation happened during the visual cryptography technique. The color images used by media are different. The contrast of pixels and the light colors usage. The gray level in images depends on the density of dark pixels. The way of using density of pixels needed is set to be scattered and those of dark areas are more and made gray level to half tone image. The human eye can see only concentrated region in the image.

Two models are used in color models. First additive model and subtractive models. In additive model Red, Green, Blue which is primary colors where colors are mixed to get composite colors. When all colors are mixed with equal wavelength (Red Green and Blue) obtain white color. Modulate the color Red, Green so we get different components of colors. The different colors which we get by mixing will add up the brightness of light. The compound color produces colors where more brightness is produced. The screen of computer is additive system. The other colors we see is combinations of primary colors. If we paint a wall with green color it will emit and blue color will absorb colors during natural sunlight.

While using computer the software‟s are of provided with image processing software‟s. The operating system are inbuilt itself with RGB color model. Here the screen of computer is output. The human retina identifies the RGB colors.

RGB color represents 0 to 255 color bits. Its 8 color bit each.

(0,0,0) represent black and (1,1,1) represent white. In Visual cryptography the using of shares we can makes the relationship between the complementary colors (Cyan, Magenta, Yellow) which are in the subtractive model. This visual cryptography can be identified using half tone and grey color visual cryptography methods. The original image pixels and these are RGB pixel measures. Every pixel in the image is enhanced as shares. The shares of RGB image shares having RGB color components which are separated and also depend on the color image. The encryption of image is decided how much of shares are need to be generated.

The random grid based visual sharing scheme which help deal with general access structure and visual quality of reconstructed image .This paper proposes the security of proposed scheme and using generalized random visual secret sharing scheme quality of image in different situations. Analyzing the contrast of light in image in detail. They finally prove proposed method where optimal light contrast is minimal. The second part was proving the efficiency in the construction of the image without loss in quality. Here the image quality of reconstructed image are compared with Wu and Sun‟s scheme

In extended visual cryptography scheme a color images which was introduced by Droste. In a work for sharing a color images two extended visual cryptography was proposed. A 3 meaningful shares are proposed where it contains R,G ,B components of extended image. These three shares required for recovering original image and second method was two shares required for recover secret images. The components RG GB and RB contains secret image. The proposed method is made meaningful for increasing security where a cover image is also added with shares. The proposed technique in this paper is lossless in nature. The dimensions of cover images and of secret image and reconstructed images are same.

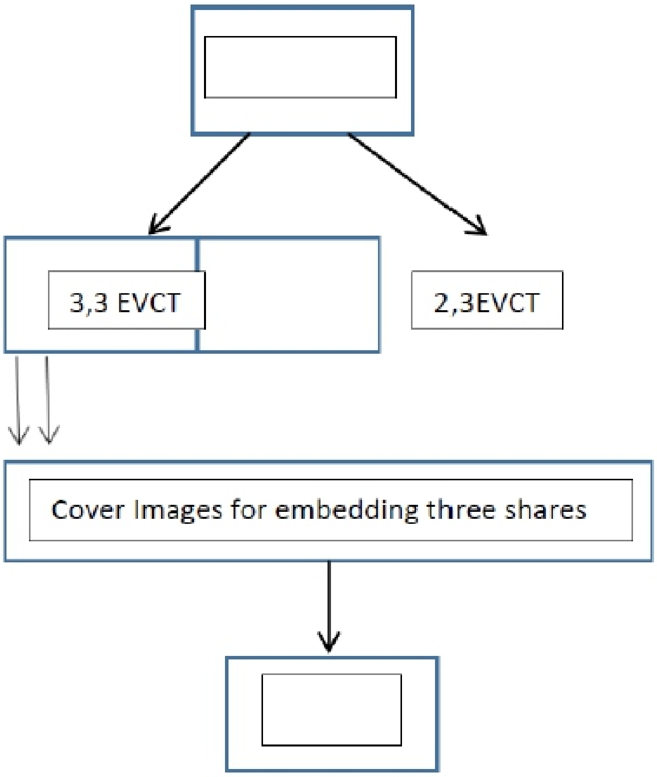


Fig.4: Extended Visual Cryptography for color images

The 3,3 EVCT and 2,3 EVCT are the two techniques to share color image. Here RGB image which is 24 bit made into 8-bit R G B components share using color decomposition. These are binded with the cover images to make them meaningful. These image shares are send to the communication medium. Every share contains 2 out of 3 components. RG, GB and RB share are created other than R, G,B shares. Hence 2,3 EVCT can produce original image. Error diffusion technique is used for high quality of visual data. The reconstructed images effectiveness are considered are on parameters such as total number of colors present in secret image. Operations performed on decryption side. Execution time for running the techniques and recovered images is lossy or not. The dimension of the image used in this experiment and applying the proposed techniques with high dimension images can also be analyzed. These techniques can be extended to general extended visual cryptography.

In chaos based visual cryptography the pixel position are used to generate the shares. This is done by using chaotic mapping where pixel values along with pixel positions are used.

In visual cryptography schemes sometimes fake shares can be inserted and remain a challenge. To avoid this XOR based visual cryptography scheme was proposed. To enhance the security these shares can be again encrypted by conventional encryption algorithms. These shares can be easily be retrieved at receiver side with fast execution and minimal peak signal noise ratio. Some visual cryptography water marking technique is used for security. The public key cryptography like RSA algorithm is used for encrypting the image shares. This is for transmitting image shares more securely.

The progressive visual cryptography by stacking more image shares. The original image can be recovered only when more shares are binded together progressively. Here if we shadow images are binded together secret image cannot be identified which can be a security advantage in case of constructed threshold visual cryptography.

In multiple image visual cryptography, when image shares are produced in correlative matrices which is used to encode the binary secret images where each pixel corresponds to block and each block extended to form n x n pixels.

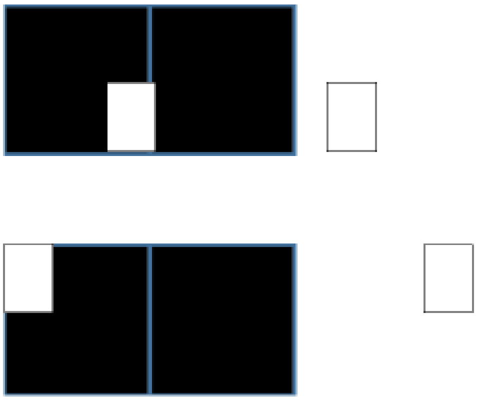


Fig.5:4 Different patterns of secret sharing

The extended block in the share will choose any of the patterns in the figure .This visual cryptography can hide more than one secret but contrast loss, security is issue. It have limits because here the image shares are square type the rotation angle is 0, 90,180, 270 only. Some changes in multiple secret sharing were done to overcome the limitation such as recursive visual cryptography. In recursive visual cryptography system images is made into shares and sub shares based on recursion. The security can be enhanced using recursion.

In the below tree representation of 2 out 2 visual cryptography system with recursion it involves two levels of encryption. S which is reconstructed by stacking shares in many ways

$$S = I1 + I2$$

$$S = I1 + I21 + I22$$

$$S = I2 + I11 + I12$$

$$S = I11 + I12 + I21 + I22$$

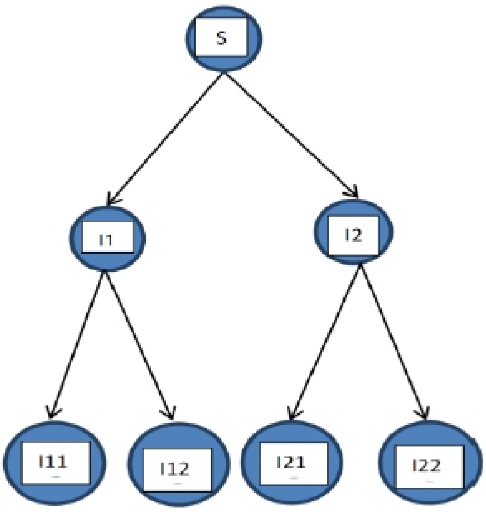
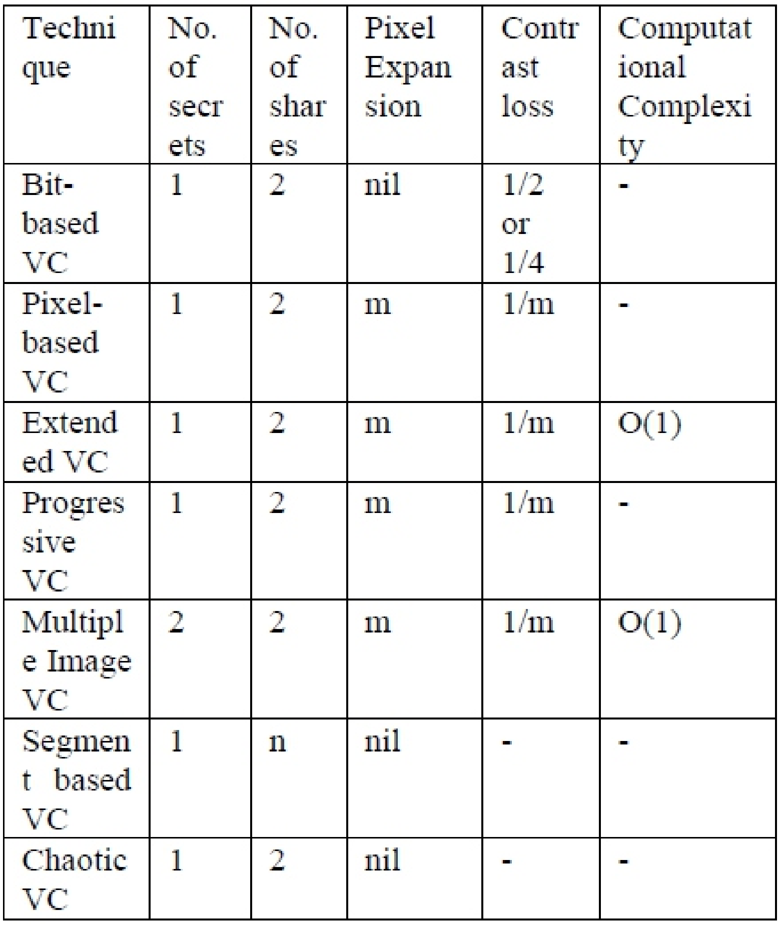


Fig.6:Two level of encryption for constructing Shares

The VCS using the many levels of encryption, the reliability and security can be improved. Here the first share is encrypted and second shares level is also again encrypted.

In segment based VC hiding message using numbers with seven segment display. The main importance in seven segment display the symbols are easily recognizable. The segment in seven segment display represented as Sn. The shares have no idea of hidden secret digit.

At the decryption side of visual cryptography the image shares are superimposed one with the other to recover the hidden secret image. There is XOR-based and OR-based VC. The shares which are produced based on OR-based VC where the pixel based which was used earlier. This is used because the reconstructed images are recovered from less number of shares. The quality of image is not degraded. Later when more shares started using the reconstructed image becomes darker. In XOR-based VC(Wu &Sun,2013) where the shares are superimposed to produce a good quality image. The XOR-based VC are commonly used logical operations at the receiver side.



Technique	No. of secrets	No. of shares	Pixel Expansion	Contrast loss	Computational Complexity
Bit-based VC	1	2	nil	1/2 or 1/4	-
Pixel-based VC	1	2	m	1/m	-
Extended VC	1	2	m	1/m	O(1)
Progressive VC	1	2	m	1/m	-
Multiple Image VC	2	2	m	1/m	O(1)
Segment based VC	1	n	nil	-	-
Chaotic VC	1	2	nil	-	-

Table 1: Different VC comparison based on parameters

The table represents the comparison between different visual cryptography. When the secret image reconstruction happens the black pixels in shares representing white pixels affect contrast loss. The size of shares used for generated by pixel based VC is directly proportional to the sub-pixels number in reconstructed image is termed as pixel expansion. The image reconstructed and having pixel expansion then size will be bigger for secret image which requires more storage space. The change in pixel intensity will affect the security. The time required for execution during the decryption must be small. So reducing the pixel expansion and contrast loss is important in visual cryptography. The strength of these techniques must be justified against histogram analysis, structural similarity index and bit error rate etc .Bit error rate is ratio between number of bit transmitted and received. Structural similarity index is the measure to find the alteration of structural information held by interdependent closed pixels and value lies between -1 to 1 .This helps about the objects in visual scene. Some of the images for transmission requires on the security aspect. The spatial image of region which have implications on security of a country. The threats can happen on both ways. The visual cryptography has various applications one is biometric privacy. The fingerprint and Iris are commonly used security feature for person. Visual cryptographic techniques are used to store and safe access into the official space and work. In probabilistic VC the pixel expansion is focused which is arising from the pixel based VC. The contrast in the recovered secret image is same as that of pixel based. Each of the pixels represent an image stored in computer as 1 bit number and common pixel format is the byte image where number stored as 8-bit ranging from 0 to 255.In intensity histogram pixel in the image at different intensity value. Some intrinsic characteristics of the image such as bulk data capacity and correlation in pixels traditional encryption like DES and IDEA not used. In flip-based visual cryptographic scheme two shares are encrypted into 2-dual based purpose shares where secret image is recovered from 2 transparencies. By flipping the one of 2 shares and binding with other share, second secret image is recovered. This scheme has optimal contrast and no pixel expansion.

Naor and Shamir proposed visual cryptography scheme. Initially the scheme was (2 ,2)-visual cryptography technique where 2-out-2 shares are reconstructed with the original image. The once which are shares are encrypted shares. The shares which are single cannot expose information in secret image. In each pixel can be expanded into many sub-pixels. It will have m sub-pixels after expansion. The (k,n)-visual cryptography technique the color image and gray scale images by lattice based concept. The color images with C distinct colors shared using this technique. The (k,n) concept for color image have C subset in the finite lattice considered as pixels which corresponds to shares. The Naor and Shamir technique extended using linear programming for increasing the color contrast of the resultant images.

The improved security feature in extended visual cryptography by having the shares meaningful. The image shares are embedded by cover image to prevent the chaos created by something in secret image. The binary images where 2 white and 2 black sub pixel block and black pixel from cover images expanded to one white and three black sub pixels. When images are recovered block which correspond to black have 4 black sub pixels and block which points to white the final image as one white and three black pixels. The contrast lost by shares half the percent of image and recovered image by 75%.

The extended visual cryptography technique was improved by taking pixel from original image. These shares have 5 white and 7 black pixels of cover image accordingly. The block is 3x3 sub pixels in share images.

In gray scale images where Chang proposed the technique where size of the image shares does not change as per the color changes in image.

The proposed techniques where k, n visual cryptography technique for color and gray-scale images uses half-toning technique .These will reduce the contrast of the color image.

The threshold visual cryptography proposed by Chao and Lin using CMY color decomposition. The 24 bits true color original image is changed into 3 bit CMY halftone image. The 3 bit halftone image is made into 2 x 2 block which is based on concept of vectors. All pixels of 3 bits halftone C-M-Y images which are processed and the image shares are constructed. 2 out of 3 image shares construct the original image. The disadvantage of this technique is that resultant secret image is noisy and lossy in nature.

The other halftone visual cryptography proposed in where making m colored halftone image shares. The quality of image is high with less noise.

The k,n visual cryptography technique based on qualified subsets where any subset group G shares images with m persons share each a distinct secret. Its said that every subset is qualified. The constructed subset will have minimal pixel expansion and good contrast.

The proposed extended visual cryptography algorithm for 4 colored images as input and constructs any 3 images which are related to images given as input. During the stacking the 3 images are binded to get fourth image. The size is the same during decryption and the constructed image shares are meaningful.

Lou proposed a method in which visual cryptography can be used by using a watermark where this can be developed using a secret and public image. A certified authority registers with secret image. Using XOR operation the watermark is developed. The proposed (3,3) and (2,2)- extended visual cryptography for sharing secret images its extension of traditional visual cryptography. The gray-scale covers are embedded into them. The binding of shares reveals original image.

Shyong and Ming proposed integer linear programming for (k,n) VCS. The generalized visual cryptography system helps with minimal optimal expansion. In this a generalized integer linear programming constructs general visual cryptography visual system.

A (2,2) circular visual cryptography for binary images. The technique is that m secret image can be stored in circular plate at a time. Then shares are created. First share in small dimension and second share in bigger dimension (double) than first share. The first share is binded with share 1 of second secret image having dimensions bigger than first secret. Again the share 2 is constructed by combining 3rd image with first two images and the method continues until secret image are encapsulated in grid. This is turn into a circular plate until final shares are constructed. Decryption of image starts when largest dimensions is extracted firstly followed by the image which is half the dimension until the method is continued secret image is found out. As seen the explanation its clear about that the proposed algorithm can handle the images of various categories and images. The sizes of image also based in the encryption phase.

In the context of cryptography security in extended visual cryptography system the conflict by dissolving the multiple images to retrieve the original image from the given images This may spoil the result as a part of quantization error where the information from the sheet and target can interact with each other because of high frequency of conflict. But human high level visual system retains only ability to understand the image recovered from originals. This will become the scheme not secure. These can be addressed by experimenting on the contrast enhancement and analyzing the image quality resulting output images. The security based on the image where the trade-off between contrast enhancement and the security of the images. The extend to this scheme to color images where color images separated in channels of primary colors red, green, blue which can be treated as independent gray scale for each color channel.

In a very naive approach, the system applies the encryption to each channel and merges the result to get the colored output. Under the ideal subtractive color mixing model, stacking the two colored sheets reveals the colored target1. In reality, however, such ideal subtractive color mixture is unlikely due to the properties of ink, transparencies, etc. It needs to establish a sophisticated color mixing model for the extended visual cryptography with better color quality.

Visual cryptography helps to secure the shares of the image. Particle swarm optimization algorithm is one of the optimization algorithms which optimize the value in the complete solution space. The particle swarm optimization based on the size of cluster for knowledge sharing in solution. In local PSO the solution the position of particle in local cluster and differs from particle. In global iteration is performed for updating of position of particle. Each particle which is part of cluster are depicted as solution which is optimize solution for new group of particles. In a network every particle can be identified which can be a structure. In ring structure every adjacent particle which decides the speed of network for deciding new velocity. In cluster similar properties of particle are communicated by particle head and it acts the root of that cluster for the the individuals in that cluster. In a big network the particles which depict the best approach globally other than taking a local approach. The encryption side in visual cryptography for the shares. Other approach is differential evolution. The differential evolution genes decide the design in population It gives most relevant solution from a complete solution. In an image the primary colors like red green blue are chromosome. Here the new images are formed from the same image using existing images .Mutation in this images can helping generation of new image.

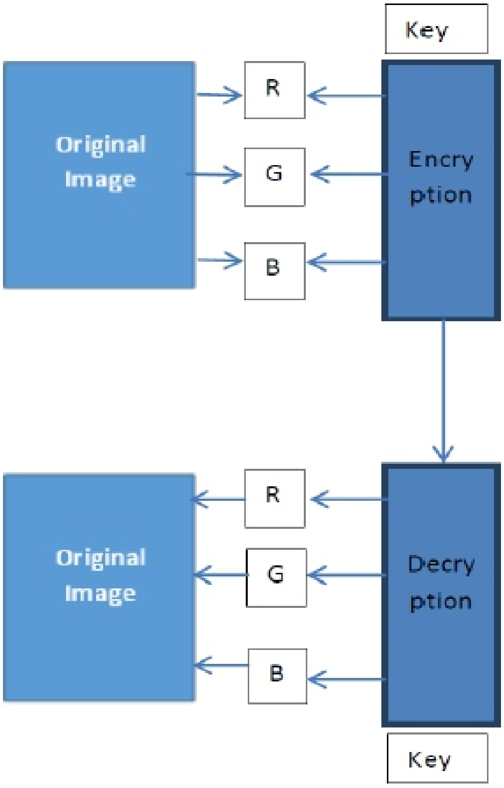
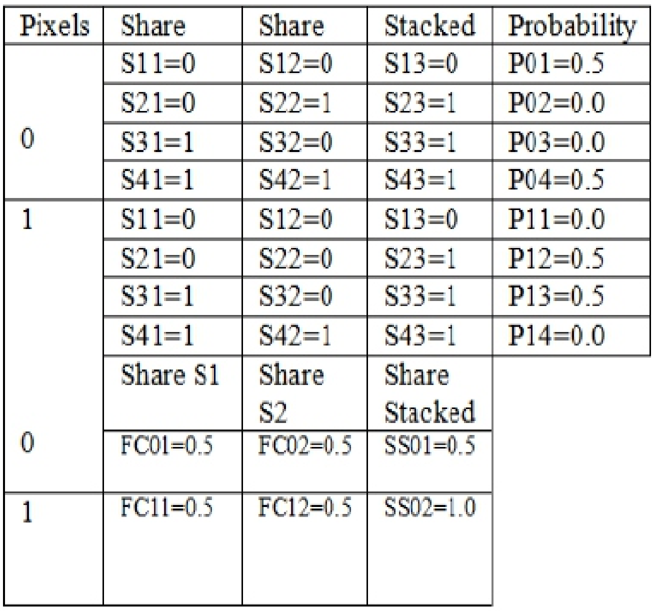


Fig.6: RGB shares secured transmission using a key

The original image which is spitted into three shares of RGB shares and encrypted. The encryption using a visual cryptography technique and a secret key generated by particle swarm optimization and encrypted by any cryptographic algorithm. The images are transmitted to the side of receiver. The key which is generated using optimization algorithm. In particle swarm optimization approach new images are formed where if differential evolution used for mutation of the particles. The values of color pixel are separated as RGB and the values from 0 to 255 are normalized. The encryption which is done by using best particle from resultant solution. The secret key obtained from final solution is used for encryption. The image shares are transmitted to receiver. The encrypted shares which constitute RGB colors are decrypted by the secret key and by superimposing all the image shares we get original image. Securing the sharing using the visual cryptography with the properties of conventional encryption of cryptography makes it harder to get the image which is divided and stored the match with a query. The original image is retrieved by superimposing the random images in regular manner. To decrease the time complexity multi thread approach is used. The individual encryption of components in image (RGB) increases the encryption. In visual cryptography the security is a hard task. The pixel expansion reduction in pixel expanded techniques can be optimized and improved in some extent. The number of individuals increasing the expansion spike exponential. The storage space, the share transmission and the computation complexity as a result.

A genetic algorithm which was proposed by Holland in 1970.GAs is composed of chromosomes which represent a solution for a problem. A genetic algorithm uses solution for analyzing and best in the evaluation searching. The reproduction, crossover and mutation is the methods used by genetic algorithm. The reproduction method uses the chromosomes which is more durable is used in solution for genetic operations. The crossover used for exchanging the genes between two chromosomes to develop offspring. The mutation method for genetic alteration randomly. Therefore the genes which are suitable for present solution to the problem will happen in new solutions. The image half toning in region of binary image higher density because of the evenly distributed black pixels. The region becomes denser due to the degree of blackness. The probability of controlling the pixel in image help without a pixel expansion. The decryption process in visual cryptography where the human eyes can understand the difference in the black and white pixels from original image and superimposed image. If change in the rules of encryption it will make a difference in black and white spaces on the shares which are not identical



Pixels	Share	Share	Stacked	Probability
0	S11=0	S12=0	S13=0	P01=0.5
	S21=0	S22=1	S23=1	P02=0.0
	S31=1	S32=0	S33=1	P03=0.0
	S41=1	S42=1	S43=1	P04=0.5
1	S11=0	S12=0	S13=0	P11=0.0
	S21=0	S22=0	S23=1	P12=0.5
	S31=1	S32=0	S33=1	P13=0.5
	S41=1	S42=1	S43=1	P14=0.0
	Share S1	Share S2	Share Stacked	
0	FC01=0.5	FC02=0.5	SS01=0.5	
1	FC11=0.5	FC12=0.5	SS02=1.0	

Table 2: Probability for analyzing security and contrast

These tables are example for probability setting for good contrast and security. If changes are made in probability setting in the encryption of the image shares there will be a difference between black and white shares. The shares FC01=S11 x P01+S21 x P02 + S31 x P03 + S41 x P04 = 0.5 this shows the probability that a white pixel is encrypted as black pixel in S1 share. Here FC01=FC11=0.5 security is ensured. The FC is the probability where white pixel is encrypted and binded as a black pixel on the stacked share of forbidden set. The contrast of stacked probability that a white pixel encrypted and stacked as black pixel SS01 = S13 x P01 + S23 x P02 + S33 x P03 + S43 x P04 =0.5 and probability a black pixel is binded and encrypted as black pixel is 1.The main objective is to find the probability when contrast of stacked share is made optimized. Chromosomes are made of series of real numbers. The real parameter is used for avoiding the loss in precision by encoding method. Binary tournament selection method it picks two chromosomes with fitness values and chromosome with higher fitness value.

The visual cryptographic methods try to expand pixels and each share size become larger than original image. The distortion of shares also needs huge space. This will be leading to the difficulty in transmission of these shares and more requirements for storage. The probability concept was used for contrast issue for constructing an optimization model.

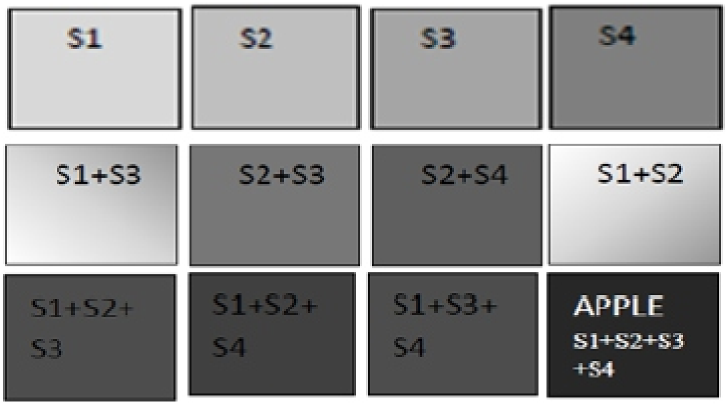
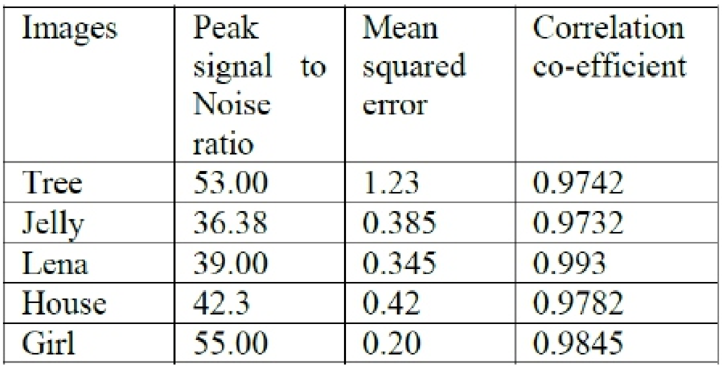


Fig.7: Probability concept for different stacked shares

From observing the above figure, It is much secure and it is easy to recognize the hidden information from the stacked shares. While using the probability model there is reconstruction of black pixels during the stacking. This is done in four shares of images. In the multiple images how much the probability model help to optimize and produce good results must be identified.



Images	Peak signal to Noise ratio	Mean squared error	Correlation co-efficient
Tree	53.00	1.23	0.9742
Jelly	36.38	0.385	0.9732
Lena	39.00	0.345	0.993
House	42.3	0.42	0.9782
Girl	55.00	0.20	0.9845

Table 3: Performance analysis of different standard test images

The table represents the performance in a system with attacks. This explains about the PSNR measure which is defined proportion of signals maximum availability to that of noise. Mean square error is average error in the occurrence in specific images. Correlation co-efficient which have two variables after encryption it will have higher correlation and identical when the correlation is 1 .This represents the hiding of information is failed .When the correlation coefficient is 0 it show major difference from the characteristics of original image.

In a digital water marking method to get meaningful number of shares generated and also achieves more security. The water marking avoid active attack because it will not give idea about the original image. This method does not cause pixel expansion

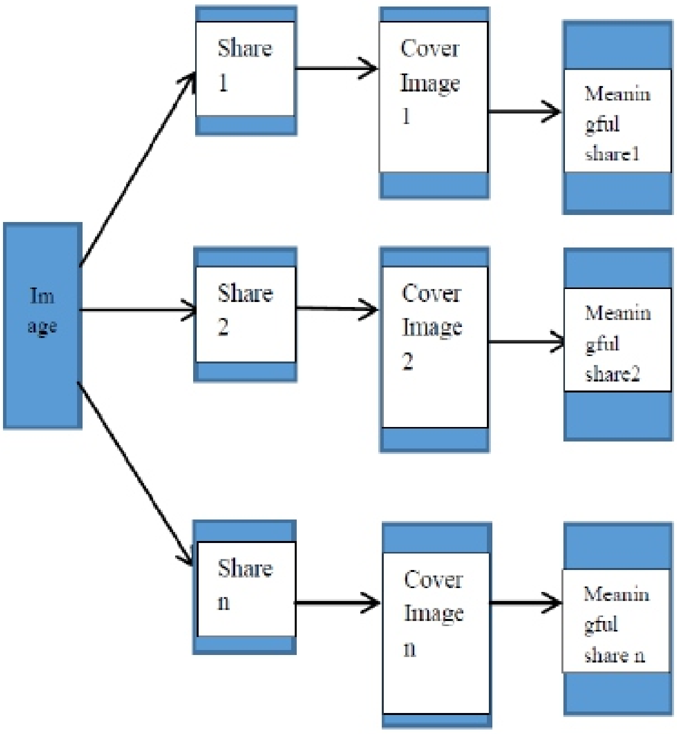


Fig.8: Securing multiple image shares using digital water marking

The original image is tested with the watermarked image. The optimal number of shares decided based on the Structural similarity, Peak signal to noise ratio, Mean Squared error. Mean squared error is done to find if the two images are same. Peak signal ratio is test for signal strength. Sometimes a possible attack on a watermark image changes the behavior of image this is identified by robustness of the image. When an image is made into three colors by decomposition C,M,Y . The digital water marking to shares avoids the identification about the original secret image.

In water marking algorithms the encoding of the source image or text is done using a secret key. This key is also used in the decoding side for gain the information source. The above figure represents the water marking embedding scheme. A typical water marking algorithm must have properties of capacity, imperceptibility and security. Capacity means the number of bits a water marking algorithm can embed in source data.

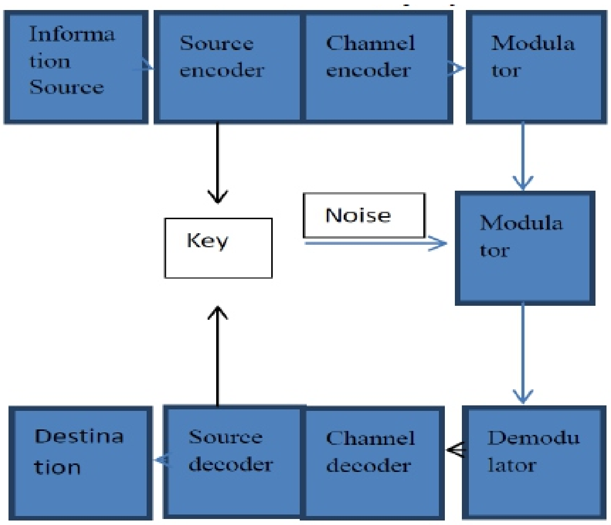
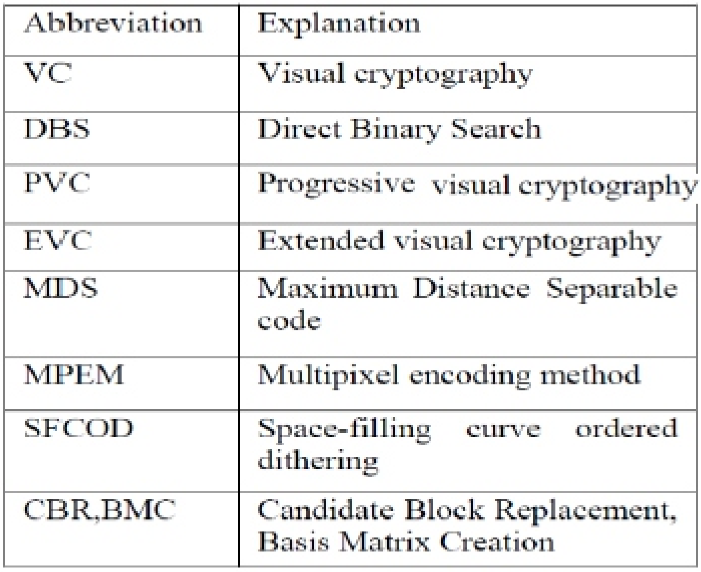


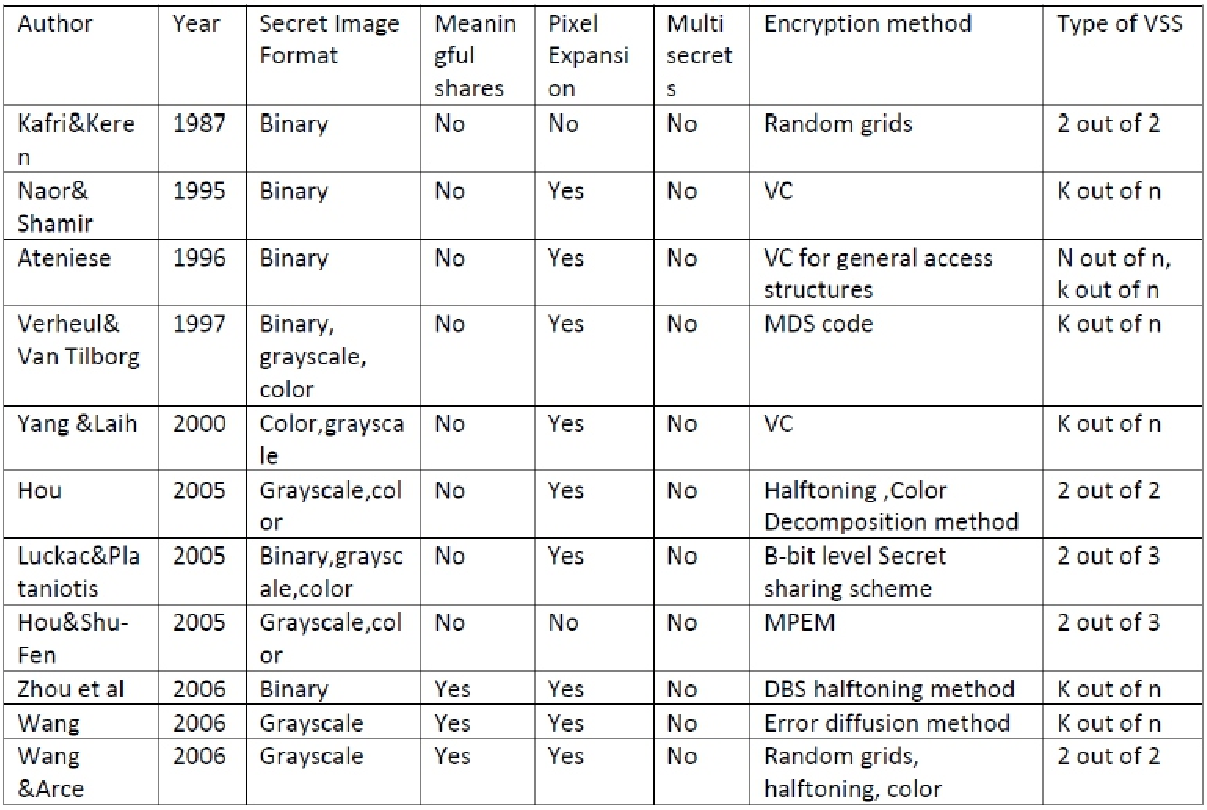
Fig.9 :Water marking encoding and decoding

The security depends where the water marking can help protecting the source data. The other property is robustness. This was about how watermark helps in preventing attacks. The robustness is important feature of water marking. The digital water marking is having three phases creation of watermark, encoding phase and decoding part for authentication. The meaningful shares that is generated for achieving the security. The watermarked shares will avoid the noise or hackers from getting the original secret. In visual cryptography multiple image secret sharing schemes water marking system is used. In progressive visual cryptography for meaningful shares and unexpanded shares the water marking methodology is used for security. The optimization algorithms involved in improving the performance and cost had helped to reduce the computation complexity involved in decryption side. The evolution and improvement of different visual cryptography schemes is illustrated in table.



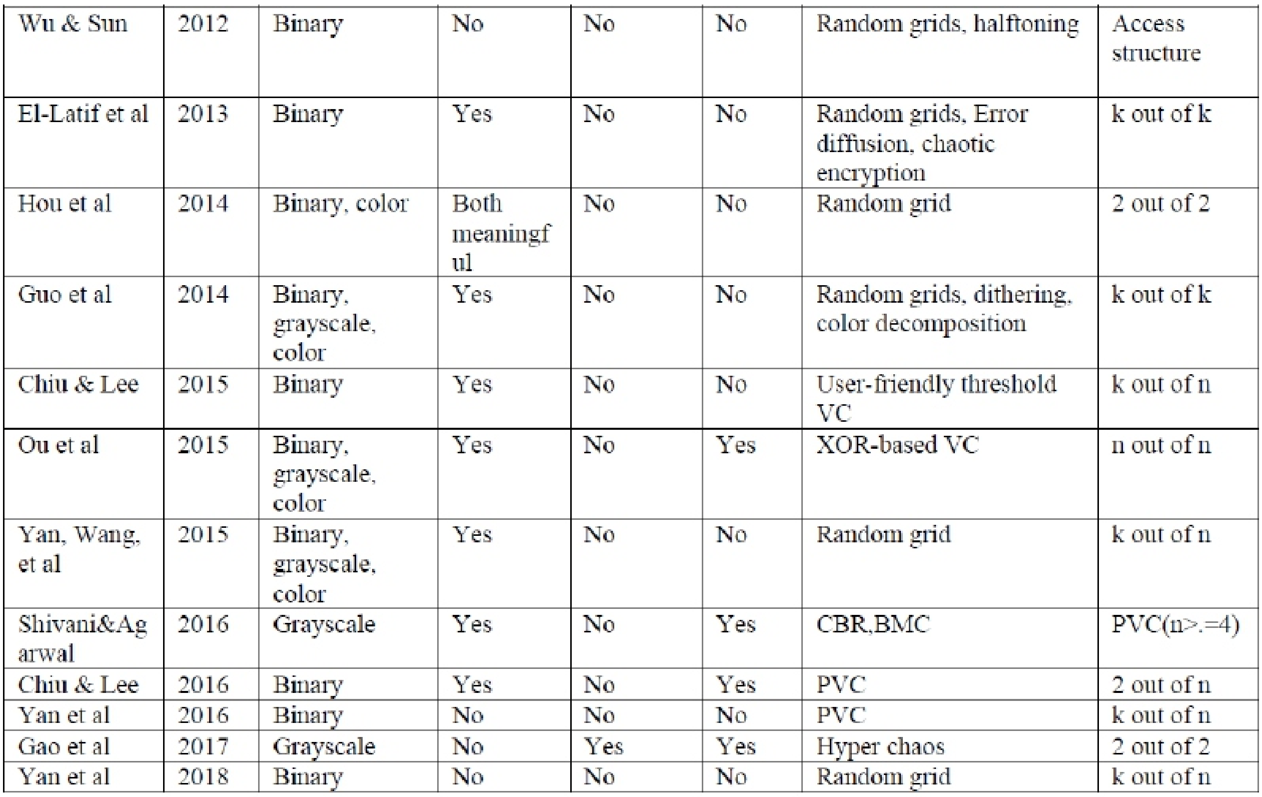
Abbreviation	Explanation
VC	Visual cryptography
DBS	Direct Binary Search
PVC	Progressive visual cryptography
EVC	Extended visual cryptography
MDS	Maximum Distance Separable code
MPEM	Multipixel encoding method
SFCOD	Space-filling curve ordered dithering
CBR,BMC	Candidate Block Replacement, Basis Matrix Creation

Table 4: Abbreviation used in Table 5



Author	Year	Secret Image Format	Meaningful shares	Pixel Expansion	Multi secrets	Encryption method	Type of VSS
Kafri&Keren	1987	Binary	No	No	No	Random grids	2 out of 2
Naor& Shamir	1995	Binary	No	Yes	No	VC	K out of n
Ateniese	1996	Binary	No	Yes	No	VC for general access structures	N out of n, k out of n
Verheul& Van Tilborg	1997	Binary, grayscale, color	No	Yes	No	MDS code	K out of n
Yang &Laih	2000	Color,grayscale	No	Yes	No	VC	K out of n
Hou	2005	Grayscale,color	No	Yes	No	Halftoning ,Color Decomposition method	2 out of 2
Luckac&Plataniotis	2005	Binary,grayscale,color	No	Yes	No	B-bit level Secret sharing scheme	2 out of 3
Hou&Shu-Fen	2005	Grayscale,color	No	No	No	MPEM	2 out of 3
Zhou et al	2006	Binary	Yes	Yes	No	DBS halftoning method	K out of n
Wang	2006	Grayscale	Yes	Yes	No	Error diffusion method	K out of n
Wang &Arce	2006	Grayscale	Yes	Yes	No	Random grids, halftoning, color	2 out of 2

Shyu	2007	Grayscale, color	No	No	No	Random grids	N out of n
Chen, Tsao& Wei	2008	Grayscale, color	No	No	No	Random grids, Halftoning	2 out of 2
Chen, Tsao& Wu	2008	Binary, grayscale	No	Yes	Yes	Multi-secret VSS	2 out of 2
Shyu	2009	Binary, grayscale, color	No	No	No	Random Grids	N out of n
Chen &Tsao	2009	Color,Binary	Yes	No	No	Random Grids	2 out of 2
Chang et al	2010	Binary	No	No	Yes	Random grids	2 ot of 2
Wang et al	2010	Binary	No	No	No	IVCRG	N level IVCRG
Prakash&Govindraju	2011	Color	Yes	No	No	DBS with adaptive search & swap	n out of n
Chen &Tsao	2011	Binary, Grayscale,color	No	No	No	FRGVSS	2 out of 2
Sharma	2012	Grayscale	Yes	Yes	No	Error diffusion method	2 out of 2
Hsu &Jua	2012	Binary	No	Yes	No	Random grids	2 out of 2
Chang & Juan	2012	Binary	No	No	Yes	Shifting random grids	2 out of 2
Wu & Sun	2012	Binary	No	No	No	Random grids, halftoning, color	Access structure
El-Latif et al	2013	Binary	Yes	No	No	Random grids, Error diffusion, chaotic encryption	k out of k
Hou et al	2014	Binary, color	Both meaningful	No	No	Random grid	2 out of 2
Guo et al	2014	Binary, grayscale, color	Yes	No	No	Random grids, dithering, color decomposition	k out of k
Chiu & Lee	2015	Binary	Yes	No	No	User-friendly threshold VC	k out of n
Ou et al	2015	Binary, grayscale, color	Yes	No	Yes	XOR-based VC	n out of n
Yan, Wang, et al	2015	Binary, grayscale, color	Yes	No	No	Random grid	k out of n
Shivani&Agarwal	2016	Grayscale	Yes	No	Yes	CBR,BMC	PVC(n>.=4)
Chiu & Lee	2016	Binary	Yes	No	Yes	PVC	2 out of n
Yan et al	2016	Binary	No	No	No	PVC	k out of n
Gao et al	2017	Grayscale	No	Yes	Yes	Hyper chaos	2 out of 2
Yan et al	2018	Binary	No	No	No	Random grid	k out of n
Hsu &Jua	2012	Binary	No	Yes	No	Random grids	2 out of 2
Chang & Juan	2012	Binary	No	No	Yes	Shifting random grids	2 out of 2



Wu & Sun	2012	Binary	No	No	No	Random grids, halftoning	Access structure
El-Latif et al	2013	Binary	Yes	No	No	Random grids, Error diffusion, chaotic encryption	k out of k
Hou et al	2014	Binary, color	Both meaningful	No	No	Random grid	2 out of 2
Guo et al	2014	Binary, grayscale, color	Yes	No	No	Random grids, dithering, color decomposition	k out of k
Chiu & Lee	2015	Binary	Yes	No	No	User-friendly threshold VC	k out of n
Ou et al	2015	Binary, grayscale, color	Yes	No	Yes	XOR-based VC	n out of n
Yan, Wang, et al	2015	Binary, grayscale, color	Yes	No	No	Random grid	k out of n
Shivani&Agarwal	2016	Grayscale	Yes	No	Yes	CBR,BMC	PVC(n>.=4)
Chiu & Lee	2016	Binary	Yes	No	Yes	PVC	2 out of n
Yan et al	2016	Binary	No	No	No	PVC	k out of n
Gao et al	2017	Grayscale	No	Yes	Yes	Hyper chaos	2 out of 2
Yan et al	2018	Binary	No	No	No	Random grid	k out of n

Table 5: Different type of visual cryptographic techniques

IV. CONCLUSION

In the network we discuss about the different type of attack. The attack which is very unable to trace is passive attack. This does not require any software or any algorithm for gaining the information. The amount of data especially multimedia data which is transmitted through network has a amount of loss due to the various factors which was discussed in this paper. This paper also discuss about visual cryptography. After analyzing from table there are more number of visual secret sharing schemes are being available and developed over the years. The amount of data that is transferred through network is huge. The concern for secure transmission of data is biggest challenge. The method to protect the multimedia data from unauthorized person is a threat for the distribution and major disadvantage for the business related to IT industry. The images that are used for encryption during the transmission require security with less decryption time. This will help for less computation complexity and also the cost of implementation of visual secret sharing scheme in a large network. There are many visual secret sharing schemes which is used for different purposes in real time environment. The visual cryptography techniques with different performance parameters are identified such as pixel expansion, quality of shares, size, visual quality recovered image, contrast, size of the image, computational complexity and number of shares generated for different visual cryptographic techniques.

REFERENCE

[1] Ateniese, G., Blundo, C., De Santis, A., & Stinson, D. R., " Visual cryptography for general access structures", Information and Computation, 129(2), 86–106. doi:10.1006/inco.1996.0076,1996

[2] Ateniese, G., Blundo, C., De Santis, A., & Stinson, D. R., "Extended capabilities for visual cryptography.", Theoretical Computer Science 250(1–2): 143–161. doi:10.1016/S0304- 3975(99)00127-9,2001

[3] Chao, H. C., & Fan, T. Y., "XOR-based progressive visual secret sharing using generalized random grids", Displays, 49, 6–15. doi:10.1016/j.displa.2017.05.004, 2017

[4] Chen, T. H., &Tsao, K. H., "Visual secret sharing by random grids revisited", Pattern Recognition, 42(9), 2203–2217. doi:10.1016/j.patcog.2008.11.015

[5] Chen, T. H., &Tsao, K. H.," Threshold visual secret sharing by random grids ", Journal of Systems and Software, 84(7), 1197–1208. doi:10.1016/j.jss.2011.02.023,2011

[6] Chen, T. H., &Tsao, K. H., "User-friendly random-grid based visual secret sharing" , IEEE Transactions on Circuits and Systems for Video Technology, 21(11), 1693–1703. doi:10. 1109/TCSVT.2011.213347

[7] Chen, T. H., Tsao, K. H., & Lee, Y. S, "Yet another multiple-image encryption by rotating random grids", Signal Processing, 2012. doi:10.1016/j. sigpro.2012.02.015

[8] Chiu, P. L., & Lee, K. H., " User-friendly threshold visual cryptography with complementary cover images ", Signal Processing, 108, 476–488. doi:10.1016/j. sigpro.2014.09.032, 2015

[9] Chiu, P. L., & Lee, K. H., "An XOR-based progressive visual cryptography with meaningful shares", Computer Communication and the Internet (ICCCI), 2016 IEEE International Conference on (pp. 362–365), Wuhan, China: IEEE. doi:10.3389/fpls.2016.00362,2016

[10] Carlo Blundoa, StelvioCimatob, Alfredo De Santisa., "Visual cryptography schemes with optimal pixel expansion", Theoretical Computer Science 369 (2006) 169– 182, 2018

[11] El-Latif, A. A. A., Yan, X., Li, L., Wang, N., Peng, J. L., &Niu, X , " A new meaningful secret sharing scheme based on random grids, error diffusion and chaotic encryption ", Optics & Laser Technology, 54, 389–400. doi:10.1016/j. optlastec.2013.04.018,2013

[12] Hou, Y. C, "Visual cryptography for color images. Pattern Recognition, 36(7), 1619–1629. doi:10.1016/ S0031- 3203(02)00258-3,2003

[13] Ming Wang, Bo Cheng , and Chau Yuen, " Joint Coding-Transmission Optimization for a Video

[14] Surveillance System With Multiple Cameras",IEEE Transactions on multimedia, Vol. 20, No. 3, March 2018

[15] Venkata Krishna PavanKalubandi, HemanthVaddi, Vishnu Ramineni, AgilandeeswariLoganathan, "A Novel Image Encryption Algorithm using AES and Visual Cryptography ",IEEE 2nd International Conference on Next Generation Computing Technologies, 2016

[16] P.Geetha, Dr.V.S.Jayanthi, Dr. A.N. Jayanthi, "Optimal Visual Cryptographic Scheme with multiple share creation for

[17] Multimedia Applications", Computers & Security, Volume 78, 2018, Pages 301-320

[18] Ram Gopal Sharma, PritiDimri&HitendraGarg, "Visual cryptographic techniques for secret image sharing: a review", Information Security journal : A global perspective, https://doi.org/10.1080/19393555.2019.15 67872,2019.

[19] JiaxiGu , Jiliang Wang, Zhiwen Yu , KeleShen, "Traffic-Based Side-Channel Attack in Video Streaming", IEE E/ACM Transactions on Networking,2018

[20] RinaldiMunir, Harlili, " Video Encryption by Using Visual Cryptography Based on Wang"s Scheme", 4th International Conference on Electrical, Electronics and System Engineering,ICEESE,2018

[21] Nikhil C. Mhala, Rashid Jamal, Alwyn R. Pais, "Randomised visual secret sharing scheme for grey-scale and colour images", IET Image Processing, 2018

[22] Hussain M.J. Almohri, Layne T. Watson, Danfeng (Daphne) Yao, Xinming, "Security Optimization of Dynamic Networks with Probabilistic Graph Modeling and Linear Programming", IEEE Transactions on Dependable and Secure Computing, 2015

[23] RajatBhatnagar, Manoj Kumar," Visual Cryptography: A Literature Survey ", IEEE 2nd International conference on Electronics, Communication and Aerospace Technology ICECA,2018

[24] Xiaochun Cao, Na Liu, Ling Du, Chao Li, "Preserving privacy for video surveillance for visual cryptography", 978-1-4799-5403-2/14/$31.00 IEEE 2014

[25] Santos Merino Del Pozo, Francois-Xavier Standaert, Dina Kamel, Amir Moradi, "Side-Channel Attacks from Static Power: When Should we Care? ", Automation & Test in Europe Conference & Exhibition (DATE), 2015

[26] Pei-Ling Chiu and Kai-Hui Lee, "A Simulated Annealing Algorithm for General Threshold Visual Cryptography Schemes", IEEE Transactions on Information Forensics and Security, Vol. 6, No. 3,2011

[27] Pei-Ling Chiu, Kai-Hui Lee, "Optimization Based Adaptive Tagged Visual Cryptography", GECCO"18, July 15-19, 2018,

[28] Roberto De Prisco, Alfredo De Santis, "Color visual cryptography schemes for black and white secret images", Theoretical Computer Science ,2013

[29] Ran Dubinz, AmitDvir, OfirPeley, OferHadarz, "I Know What You Saw Last Minute -Encrypted HTTP Adaptive Video Streaming Title Classification, IEEE Transactions on Information Forensics and Security,2017

[30] AbulHasnat, Dibyendu Barman, Satyendra Nath Mandal , "A Novel Image Encryption Algorithm Using Pixel

[31] Shuffling and Pixel Intensity Reversal",IEEE International Conference on Emerging Technological Trends 2016

[32] Naoki Kita, Kazunori Miyata, "Magic sheets: Visual cryptography with common shares", Computational Visual Media Vol. 4, No. 2, 2018, 185–195

[33] AlIaLevina, DariaSleptsova, Oleg Zaitsev, "Side-Channel Attacks and Machine Learning Approach " 18TH Conference Of Fruct Association,2016

[34] KirtiDhiman, Singara Singh Kasana, "Extended visual cryptography techniques for true color images " , Computers and Electrical Engineering, https://doi.org/10.1016/j.compeleceng.2017.09.017,2017

[35] Young-Chang Hou, "Visual cryptography for color images", Pattern Recognition 36 , 1619 – 1629, 2002

[36] Imon Mukherjee, RitamGanguly, "Multiple video clips preservation using folded back audio-visual cryptography scheme", Springer Science+Business Media New York 2017

[37] Xiaokuan Zhang, Jihun Hamm, Michael K. Reitery, Yinqian Zhang, "Statistical Privacy for Streaming Traffic", Network and Distributed Systems Security (NDSS) Symposium, https://dx.doi.org/10.14722/ndss. 2019.23210, 2019

[38] Ching-Sheng Hsu, Shu-Fen Tu, and Young-Chang Hou, "An Optimization Model for Visual Cryptography Schemes with Unexpanded Shares" Springer-Verlag Berlin Heidelberg,2006

[39] Allan Pintoa, William Robson Schwartzb, HelioPedrinia, and Anderson Rocha, "Using Visual Rhythms for Detecting

[40] Video-based Facial Spoof Attacks", IEEE Transactions on Information Forensics And Security, 2015

[41] P. Punithavathi , S. Geetha Visual cryptography: A brief survey, Information Security Journal : A Global Perspective, 26:6, 305-317, DOI:10.1080/19393555.2017.1386249,2017

[42] Ming Tang, MaixingLuo, Junfeng Zhou, Zhen Yang, ZhipengGuo, Fei Yan, Liang Liu, Side-Channel Attacks in a Real Scenario", Tsinghua Science and Technology, 2018, 23(5): 586–598

[43] Raphael Spreitzer, VeelashaMoonsamy, Thomas Korak, Stefan Mangard, "Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices, IEEE Communications Surveys and Tutorials,2017

[44] Shuo Chen, Rui Wang, XiaoFeng Wang, Kehuan Zhang, "Side-Channel Leaks in Web Applications: a Reality Today, a Challenge Tomorrow", IEEE Symposium on Security and Privacy,2010

[45] Bin Yan, Yong Xiang, GuangHua," Improving the Visual Quality of Size-Invariant Visual Cryptography for Grayscale Images: An Analysis-by-Synthesis (AbS) Approach, IEEE Transactions on Image Processing,2019

[46] Ching-NungYang,Dao-Shun Wang," Property Analysis of XOR-Based Visual Cryptography", IEEE Transactions On Circuits And System For Video Technology, VOL. 24, NO. 2,2014

[47] ZHAO Dongmeia,b, LIU Jinxing, "Study on Network Security Situation Awareness based on Particle Swarm Optimization Algorithm", Computers & Industrial Engineering , doi: https://doi.org/10.1016/j.cie., 2018

[48] Ross, A., & Othman A , " Visual cryptography for biometric privacy. IEEE Transactions on Information Forensics and Security, 2011

[49] Chettri L, GurungS,"Recursive information hiding in threshold visual cryptography scheme" International Journal of Emerging Technology and Advanced Engineering, 3(5):536–540, 2013

[50] Liu F, Wu C , " Embedded extended visual cryptography schemes", IEEE Transactions on Information Forensics and Security , 2011

[51] Lin SJ, Chung WH ,"A probabilistic model of (t,n) visual cryptography scheme with dynamic group." IEEE Transactions on Information Forensics and Security, doi: 10.1109/TIFS.2011.2167229,2012

[52] R. Gayathri, Dr. V. Nagarajan "Secure data hiding using Steganographic technique with Visual Cryptography and Watermarking Scheme",IEEE ICCSP conference2015

[53] Z. Zhou, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography," IEEE Trans. Image Process., Aug. 2006.

[54] Wang, D. S, Zhang, L., Ma, N., et al. "Two secret sharing schemes based on Boolean operations", Pattern Recognition, 2007

[55] Yuanfeng Liu, Zhongmin "Halftone Visual Cryptography with Color Shares", IEEE International Conference on Granular Computing (GrC), 2012

[56] Liu, F., Wu, C. K., Lin, X, "Some extensions on threshold visual cryptography schemes". The Computer Journal,

[57] Wang D. S, Yi, F, "On converting secret sharing scheme to visual secret sharing scheme ", EURASIP Journal on

[58] F. Liu and C. Wu,"Embedded extended visual cryptography schemes", IEEE Transactions on Information. Forensics Security, 2011.

[59] K.-H. Lee, P.-L. Chiu, "Sharing visual secrets in single image random dot stereograms," IEEE Transactions on Image Processing, 2014.

[60] W. Ran-Zan, H. Shuo-Fang, "Tagged visual cryptography," Signal Processing Letters, IEEE, 2011

[61] M. Iwamoto, "A Weak Security Notion for Visual Secret Sharing Schemes",IEEE Transactions on Information Forensics and Security, 2012

[62] Munir, R, "Comparison of Secret Color Image Sharing Based on XOR Operation in RGB and YCbCr Color Space", Proceeding of ICEEI, 2017

[63] KulvinderKaur , VineetaKhemchandani, "Securing Visual Cryptographic Shares using Public Key Encryption", Advance Computing Conference, Feb, 2013

[64] D.Wang, L. Dong, X. Li, "Towards Shift Tolerant Visual Secret Sharing Schemes", IEEE Transactions on Information Forensics and Security , 2011

[65] H. Abdolrahimpour, E. Shahab, "A Short Survey of Visual Cryptography and Secret Image Sharing Techniques and Applications", International Advanced Research Journal in Science, Engineering and Technology, 2017

[66] Shivani, S.: „Vmvc: verifiable multi-tone visual cryptography", Multimedia Tools Appl., 2017, https://link .springer.com/article/10.1007/s11042-017-4422-6

[67] B. Shrivas, S. Yadav, "Visual Cryptography in the Video using Halftone Technique", International Journal of Computer Applications, 2015

[68] X.Wang, "Intelligent multi-camera video surveillance: A review," Pattern Recognition, Jan. 2013.

[69] D. S. Wang, L. Zhang, N. Ma, and X. Li, "Two secret sharing schemes based on Boolean operations," Pattern Recognition, 2007.

[70] Yan, X., Wang, S., &Niu, X, "Threshold construction from specific cases in visual cryptography without the pixel expansion", Signal Processing, doi: 10.1016/j.

[71] sigpro.2014.06.011

[72] Sridhar, S, Sathishkumar R, Sudha, "Adaptive halftoned visual cryptography with improved quality and security", Multimedia Tools Appl.,2017

[73] Hou, Y. C., Wei, S. C., Lin, C. Y, "Random-grid based visual cryptography schemes. IEEE Transactions on Circuits and Systems for Video Technology", 2014

[74] doi:10.1109/TCSVT.2013.2280097

[75] M. Ulutas, G. Ulutas and V. Nabiyev, "Medical image security and EPR hiding using Shamir's secret sharing scheme", The Journal of Systems and Software, 2011

[76] Weir, J.,Yan, W, "A comprehensive study of visua cryptography. In Transactions on data hiding and multimedia security ",Berlin, Heidelberg: Springer, 2010

[77] Yan, X., Wang, S., El-Latif A, Niu, X.,"Random grids-based visual secret sharing with improved visual quality via error diffusion", Multimedia Tools and Applications,2015.doi:10.1007/s11042-014-2080-5

[78] Roberto De Prisco, Alfred De Santis, "Color visual cryptography schemes for black and white secret images", Theoretical Computer Science , 2013

ISSN NO. (Print) : 2320-2106, (Online): 2321-2063

Microprocessor Power Management based on Programming Techniques

Abdullah Alshehri
Management and Information Technology department, Jubail Industrial College, Jubail Industrial City, Saudi Arabia, 31961 E-mail: alshehri_as@jic.edu.sa

ABSTRACT

This paper presents a technique to reduce the electrical power consumption of the microprocessor. The concept is based on writing the code that uses the microprocessor components with less power consumption. The simulation was carried out for various pieces of codes such as sorting algorithms and comparison of various programming key words. The results show that bucket sorting algorithm consumes the minimum power among other sorting algorithms even it does not perform as the best in terms of execution complexity. However, when number of cores increases, bucket sorting algorithms tends to be comparable to other sorting algorithms. Other programming codes show various power consumption behaviors.

Keywords - Microprocessor Electrical Power, Power Management, Efficient Sorting Algorithms, Hotspot Cooling.

I. INTRODUCTION

Every 18 months, the number of transistors that can be packaged in a semiconductor die is doubled. This is what Moore's law sates [1]. It was held for decades. However, in recent years the challenges grow in a way that Moore's law does not hold any more. The 10 nm technology was delayed 5 years after the last microprocessor generation [2]. The challenges vary from fabricationprecision difficulty in nanometer scale to power consumption and dissipation [3]. Chip designers look for any improvement that can lead to better die packaging. With the current ability, power dissipation can be improved which can lead to increase in the packaging size while maintaining the microprocessor temperature. The dynamic power generated by CMOS integrated circuit (IC) can be approximately calculated as [4]:

$$P_{dyn}=C_{eff}V_{DD}^{2}f$$

Where C_{eff} is the effective switching capacitance, V_{DD} is the supply voltage and fis the operating frequency. To reduce the dynamic power consumption, either one or more parameters should be reduced. The effective capacity can be reduced by clock gating and sleep mode. The performance will then be affected. V can be reduced up to certain value but no huge effect can be obtained. The only possible parameter that has huge effect is the frequency. However, reducing the frequency will reduce the computation power of the system which is not preferable in the first place [5,6]. So the suggested solution is to let the power increases but reduces its effect of microprocessor temperature rising. This is done by effectively removing the heat generated by the IC using efficient cooling methods [7,8].

In this research, reducing the electrical power consumption and therefore the microprocessor temperature can be viewed from programming prospective. It is clear that some computer codes consume power than others. For example, loop with X iterations would consume electrical power less than same loop with 2X iterations. But when two different programming codes run on the same processor, it is difficult to guess which one consumes more electrical power. One can argue that the code that runs longer consumes more electrical power. It is not always true. This is because different microprocessor components consume electrical power more than others [9]. So to compare two codes, it is needed to find out what microprocessor components are involved in execution such code and for how long. Also, the execution time difference between two codes may be very small which does not give any clue on the electrical power consumption difference between the two codes.

Some of the programming codes are evaluated to discover the electrical power consumption difference among them. Sorting algorithms and comparison codes are in particular of interest.

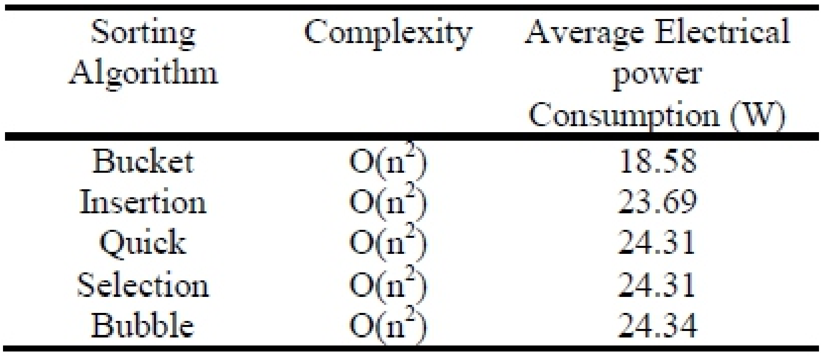
II. SORTING ALGORITHMS ELECTRICAL POWER CONSUMPTION

Sorting algorithms are widely used in programming codes. There are many sorting algorithms. Each of which has its time complexity. One would think that the higher the time complexity of the sorting algorithm the higher the electrical power consumption. In fact, it is not always true. Five sorting algorithms have been investigated in this research using hardware simulator called Sniper. Sniper is a parallel, high-speed and accurate x86 simulator. This multi-core simulator performs fast and accurate simulation exploring different homogeneous and heterogeneous multi-core architectures. The Sniper simulator allows one to perform timing simulations for both multi-programmed workloads and multi-threaded, shared-memory applications running on many cores at a high speed. The main feature of the simulator is its core model which is based on interval simulation, a fast mechanistic core model. Sniper has been validated against multi-socket Intel Core2 and Nehalem [10]. Sniper integrates with the McPAT electrical power and area modeling framework to estimate a program's electrical power consumption in a form of electrical power stacks.

The generated electrical power output data shows the electrical power usage of the application broken down by component [11]. One can choose to get dynamic, static or total electrical power, or chip area per component. It is used in this research to obtain the average electrical power consumption of various microprocessor components such as instruction fetch unit, integer unit, floating point unit, instruction catch unit and others.

Five sorting algorithms were executed using Sniper and McPAT. They were bucket, bubble, insertion, quick and selection sorting algorithms. The results show that bucket sorting algorithm consumes the least electrical power. All of these sorting algorithms has O(n2) complexity. The algorithms were written with array size of 1000.

The arrays were sorted in revered order to have similar initial condition for all algorithms. Table 1 shows the results including the complexity of each sorting algorithm.



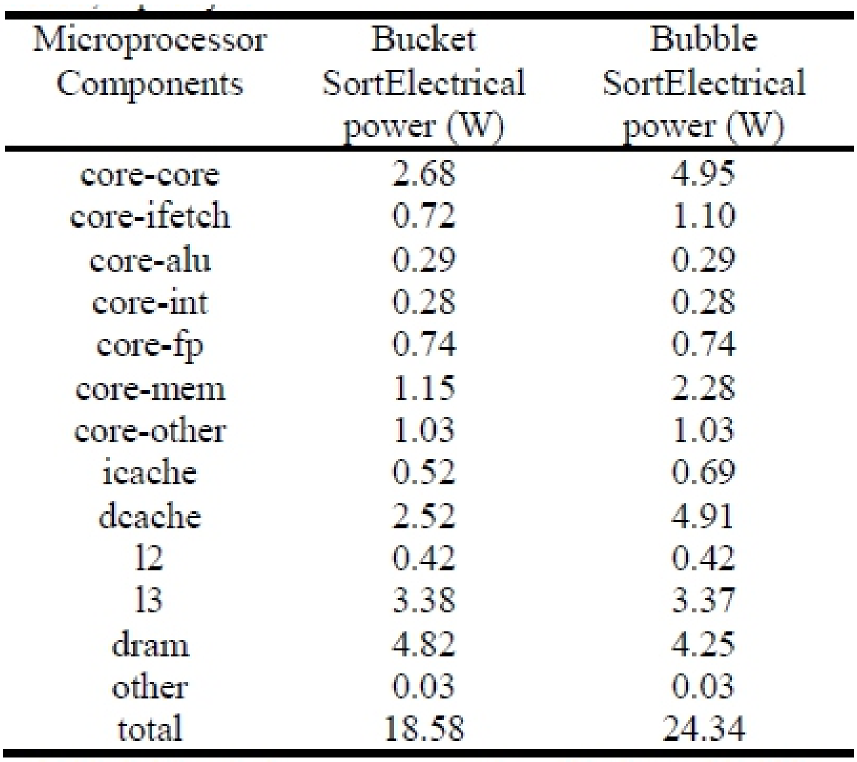
Sorting Algorithm	Complexity	Average Electrical power Consumption (W)
Bucket	$O(n^2)$	18.58
Insertion	$O(n^2)$	23.69
Quick	$O(n^2)$	24.31
Selection	$O(n^2)$	24.31
Bubble	$O(n^2)$	24.34

Table 1: Electrical power consumption of various sorting algorithms

The detailed outcomes for the simulator are shown in Table 2. When comparing bubble and bucket sorting algorithms, it is noticeable that bubble sorting algorithm consumes more average electrical power because of some microprocessor components consumes electrical power more than other such as ifetch, core-mem, icatch and some more.

The consumption is based on the fact that bucket sort uses more storage capability than bubble sort. It is not because the bucket sort uses more integer and/or floating point computation units. It is clear that bucket sorting algorithms consumes less than all other sorting algorithms while producing the same execution performance according to its complexity.

Therefore it is advised that programmers use this sorting algorithm to consume less electrical power. This is even clear when the sorting tasks are repeated many times.



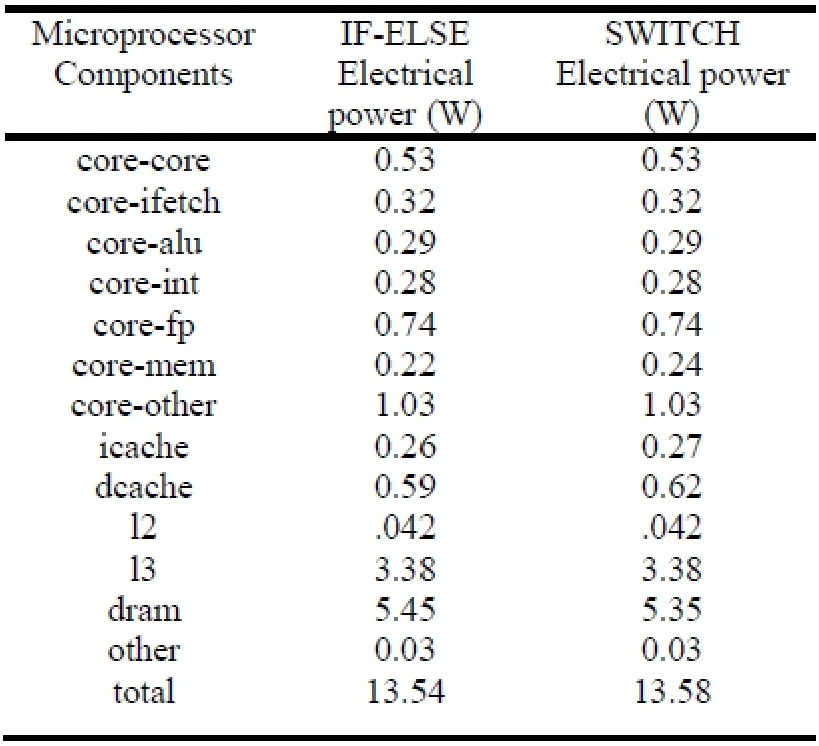
Microprocessor Components	Bucket SortElectrical power (W)	Bubble SortElectrical power (W)
core-core	2.68	4.95
core-ifetch	0.72	1.10
core-alu	0.29	0.29
core-int	0.28	0.28
core-fp	0.74	0.74
core-mem	1.15	2.28
core-other	1.03	1.03
icache	0.52	0.69
dcache	2.52	4.91
l2	0.42	0.42
l3	3.38	3.37
dram	4.82	4.25
other	0.03	0.03
total	18.58	24.34

Table 2: Electrical power consumption of Bucket and Bubble sorting algorithms

III. SWITCH AND IF-ELSE STATEMENT ELECTRICAL POWER CONSUMPTION

Comparison was made between SWITCH and IF statement. The code was written in C language. Seven switches and similar IF-ELSE were constructed. The average electrical power consumption was 13.58 W and 13.54 W for the SWITCH and IF-ELSE statement respectively.

Few microprocessor components show minor differences such as core-mem, icache, dcache and dram units. The difference is about 0.04 W. It may not be huge if the code is used once. However, if the IF-ELSE is used repeatedly, the effect will be noticeable. For example, if a piece of code containing IF-ELSE was executed 1000 times, the electrical power saving compared to SWITCH is 40 W which is huge.

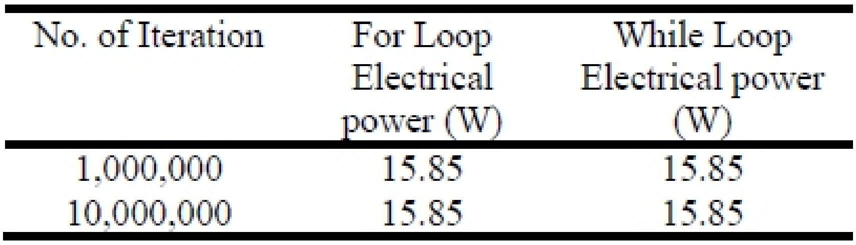


Microprocessor Components	IF-ELSE Electrical power (W)	SWITCH Electrical power (W)
core-core	0.53	0.53
core-ifetch	0.32	0.32
core-alu	0.29	0.29
core-int	0.28	0.28
core-fp	0.74	0.74
core-mem	0.22	0.24
core-other	1.03	1.03
icache	0.26	0.27
dcache	0.59	0.62
l2	.042	.042
l3	3.38	3.38
dram	5.45	5.35
other	0.03	0.03
total	13.54	13.58

Table 3: Electrical power consumption of IF-ELSE and SWITCH statements

IV. FOR LOOP AND WHILE LOOP ELECTRICAL POWER CONSUMPTION

For loop and while loop show identical average electrical power consumption. Executing both in few iterations or large number of iterations does not change the electrical power consumption behavior of both types of loops. Table 4 shows the electrical power consumption of both loops. The result is based on Sniper simulation. When using actual compilers, the result may not be the same. This concept with be investigated in future research work.



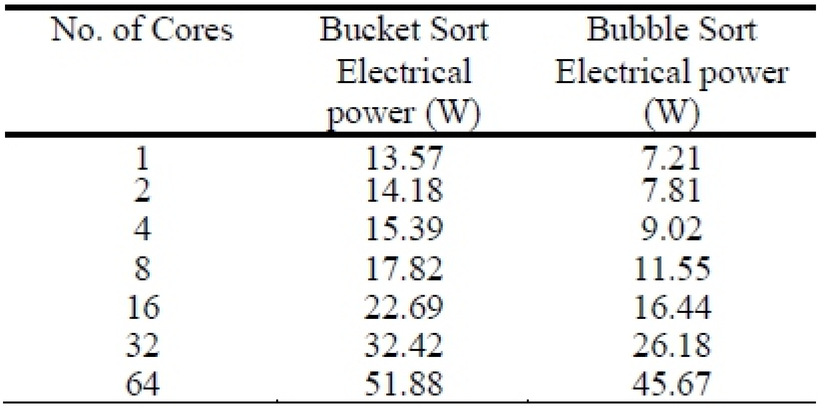
No. of Iteration	For Loop Electrical power (W)	While Loop Electrical power (W)
1,000,000	15.85	15.85
10,000,000	15.85	15.85

Table 4: Electrical power consumption of For and While loops

V. MULTICORE EFFECTS

Multicore systems solve many problem related to microprocessor speed by utilizing parallelism in programming codes. It also solves heating problem by distributing the execution load among various cores which lead to better head distribution.

It is found that when running the two sorting algorithms (bubble and bucket) on single and multi-core, the electrical power consumption comparison becomes different. When comparing bucket sorting algorithm bubble sorting algorithm for the whole microprocessor electrical power consumption, bucket sorting outperform bubble soring by almost 31% as shown in Table 1. This is when single core microprocessor is sued. However, when number of cores is increased, the electrical power consumption tends to equalize. Figure 1 shows the trend of using multicore system to execute bucket and bubble sorting algorithms. So, it is clear that the programmer can choose bucket sorting algorithm when using low number of processor. This will make the electrical power consumption minimal. However, for large number of cores, the difference in electrical power consumption between the two sorting algorithms is not huge. More research is needed to investigate the other sorting algorithms and other programming techniques such as IF and WHILE key words.



No. of Cores	Bucket Sort Electrical power (W)	Bubble Sort Electrical power (W)
1	13.57	7.21
2	14.18	7.81
4	15.39	9.02
8	17.82	11.55
16	22.69	16.44
32	32.42	26.18
64	51.88	45.67

Table 5: Cores Electrical power consumption of Bucket and Bubble sorting algorithms

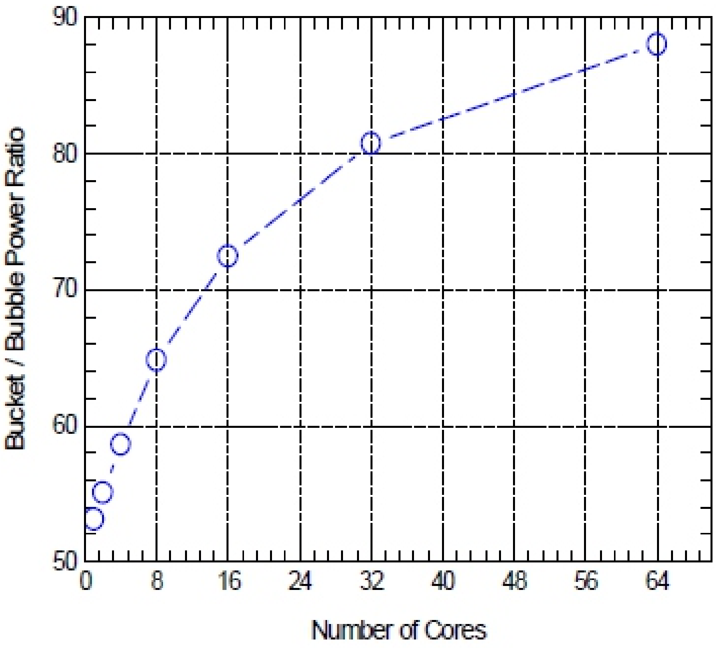


Figure 1. Bucket/Bubble electrical power ratio vs number of cores.

VI. CONCLUSION

Reducing the microprocessor electrical power consumption by choosing the proper programming technique was made possible. Various sorting and searching algorithms with equal execution complexities consume different electrical powers. For example, bucket and bubble sort algorithms have O(n2) execution complexities while bucket sorting algorithm consumes about 76% of bubble sorting algorithms. Other loop methods show different electrical power consumptions.

Running programs on multicores systems effects the electrical power consumption when compared to single core systems. Increasing the number of cores makes the difference in electrical power consumptions between bucket and bubble sorting algorithms reduced. Therefore, it is possible to reduce electrical power consumption by using choices of programming techniques without any hardware interventions.

REFERENCE

[1] G. Moore, "Cramming more components onto integrated circuits".Electronics, 38(8), 1965.

[2] D.Rotman, "We're not prepared for the end of Moore's Law", MIT technology review, 2020.

[3] N. Semiconductor, "Understanding integrated circuit package electrical power capabilities," in [Online] Available: www.national.com, http://www.ti.com/lit/an/snva509a/snva509a.pdf, Mar. 2019.

[4] M. Mackowski and M. Niezabitowski, "Electrical power Consumption Analysis of Microprocessor Unit Based on Software Realization," 20th International Conference on Control Systems and Computer Science, Bucharest, pp. 493-498. 2015.

[5] R. Jejurikar,C., Pereira and R. Gupta,"Leakage aware dynamic voltagescaling for real-time embedded systems" In: The 41st AnnualDesign Automation Conference, San Diego, CA, USA, June 7–11,2004.

[6] G. Castilhos, M. Mandelli, L. Ost and F.Moraes, "Hierarchicalenergy monitoring for task mapping in many-core systems", J.Syst.Archit. 63, pp. 80–92, 2016.

[7] Gj. Snyder, M. Soto, R. Alley, D. Koester andB. Conner,"Hot spot cooling using embedded thermoelectric coolers", Twenty Second Annual IEEE semiconductor thermal measurementand management symposium, Dallas, TX USA, 2006.

[8] M. El-Genk andH. Saber,"Composite spreader for cooling computer chip with nonuniformheat dissipation", IEEE Trans ComponPackagTechnol, 31(1), pp. 165–72, 2008.

[9] S. Lee, D. Pandiyan, J. Seo and C. Wu, "Thermoelectric basedsustainable self-cooling for fine-grained processor hot spots", In:15th IEEE Intersociety Conference on Thermal and ThermomechanicalPhenomena in Electronic Systems, Las Vegas, NV, USA,31 May–3 June, 2016.

[10] T. Carlson, T. Heirman andL. Eeckhout, "Sniper: Exploring the level of abstraction for scalable and accurate parallel multi-core simulation." In Conference on High Performance Computing Networking, Storage and Analysis (Supercomputing – SC), number 52, 2011.

[11] S. Li, J.Ahn, R. Strong, J. Brockman, D. Tullsen andN. Jouppi, "McPAT: an integrated electrical power, area, and timingmodeling frameworkfor multicore and manycorearchitectures", In: Proceedings of the42nd Annual IEEE/ACMInternational Symposium onMicroarchitecture, Dec 12–16, New York, NY, 2009.

ISSN NO. (Print) : 2320-2106, (Online): 2321-2063

Modified RSA Cryptographic Algorithm for Encryption and Decryption

[1] Dharitri Talukdar, [2] Laba Kr. Thakuria, [3] L. P. Saikia
[1]Research Scholar, Assam Down Town University, Guwahati, Assam, India
[2]Deputy Controller of Examination, Assam Down Town University, Guwahati, Assam, India
[3]Professor, Girijananda Chowdhary Institute of Management and Technology, Guwahati, Assam, India
E-mail: [1]dharitritalukdar03@gmail.com, [2]thakurialaba@gmail.com, [3]lp_saikia@yahoo.co.in

ABSTRACT

Data is any type of stored digital information. Security is about the protection of assets. Information security alludes to defensive computerized protection quantifies that are applied to forestall unapproved admittance to PCs, individual information bases and sites. Cryptography is evergreen and developments. Cryptography guarantees clients by offering convenience to the encryption of data and confirmation of various customers. Pressure is the way toward diminishing the quantity of pieces or bytes expected to speak to a given arrangement of information. It allows saving more data. Cryptography is a mainstream methods of sending crucial data in a mystery way. There are many cryptographic techniques available and among them RSA is one of the most powerful techniques. The situation of present day of data security framework incorporates privacy, genuineness, honesty, non-renouncement. The security of correspondence is a vital issue on World Wide Web. It is about secrecy, respectability, validation during access or altering of private interior record.

Keyword - Encryption, Decryption, Cryptography, Data Security, RSA Algorithm.

I. INTRODUCTION

The most widely recognized public key calculation is RSA cryptosystem utilized for encryption and decoding. It is the primary public key calculation which gives security to move and sparing of information over the organization. Security objectives for information security are Confidential, Authentication, Integrity, and Non-repudiation.

Data security delivers data protection across enterprise. Data security is a developing issue among IT associations, all things considered. To handle this developing concern, increasingly more IT firms are moving towards cryptography to secure their significant data. Notwithstanding above worries over making sure about put away information, IT associations are additionally confronting difficulties with truly expanding expenses of capacity needed to ensure that there is sufficient capacity ability to meet the association's current and future requests. Data pressure is known for reducing amassing and correspondence costs. It includes changing information of a given arrangement, called source message to information of a more modest measured configuration called code word. Information encryption is known for shielding data from listening in. It changes information of a given organization, called plaintext, to another configuration, called figure text, utilizing an encryption key. At present pressure and encryption strategies are done independently. Cryptography before the cutting edge age was viably inseparable from encryption, the transformation of data from a coherent state to obvious drivel. Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. It is hypothetically conceivable to break such a framework, yet it is infeasible to do as such by any known down to earth implies[6].

II. CRYPTOGRAPHY

The specialty of cryptography is viewed as conceived alongside the craft of composing. As developments advanced, individuals got coordinated in clans, gatherings, and realms. This prompted the development of thoughts, for example, power, fights, matchless quality, and governmental issues. These thoughts further powered the normal need of individuals to discuss furtively with particular beneficiary which thus guaranteed the consistent development of cryptography also. The foundations of cryptography are found in Roman and Egyptian developments. The significance of data and correspondence frameworks for society and the worldwide economy is strengthening with the expanding worth and amount of information that is sent and put away on those frameworks. Simultaneously those frameworks and information are additionally progressively powerless against an assortment of dangers, for example, unapproved access and use, misappropriation, adjustment, and pulverization. The covering up of data is called encryption, and when the data is unhidden, it is called decoding. A code is utilized to achieve the encryption and unscrambling. Merriam-Webster's Collegiate Dictionary characterizes figure as —a strategy for changing a content to cover its significance. The data that is being covered up is called plaintext; whenever it has been encoded, it is called ciphertext. To conceal any information two methods are principally utilized one is Cryptography other is Steganography. In this paper we use Cryptography. Cryptography is the study of securing information, which gives techniques for changing over information into confused structure, with the goal that Valid User can get to Information at the Destination. Cryptography is the investigation of using science to scramble and unscramble data.

III. BASIC TERMINOLOGY OF CRYPTOGRAPHY

Computers[3] are utilized by a large number of individuals for some reasons. for example, banking, shopping, military, understudy records, etc..Privacy is a basic issue in a significant number of these applications, how are we need to ensure that an unapproved parties can't peruse or change messages. Cryptography[5] is the change of discernible and justifiable information into a structure which can't be perceived to make sure about information. cryptography alludes precisely to the strategy of hiding the substance of messages, the word cryptography comes from the Greek word "Kryptos", that implies covered up, and "graphikos" which means composing. The data that we need to cover up, is called plaintext , It's the first content, It could be in a type of characters, mathematical information, executable projects, pictures, or some other sort of data, The plaintext for instance is the sending of a message in the sender before encryption, or it is the content at the collector after unscrambling. The information that will be communicated is called figure text , it's a term alludes to the line of "futile" information, or muddled content that no one should comprehend, aside from the beneficiaries. the information will be sent Exactly through organization, Many calculations are utilized to change plaintext into figure text. Code is the calculation that is utilized to change plaintext to encode text, This technique is called encryption, as such, it's a system of changing over decipherable and justifiable information into "negligible" information. The key is a commitment to the encryption count, and this value should be independent of the plaintext, This data is used to change the plaintext into figure text, so various keys will yield diverse code text, In the unravel side, the backwards of the key will be utilized inside the calculation rather than the key. PC security it's a nonexclusive term for an assortment of instruments intended to shield any information from programmers, robbery, defilement, or catastrophic event while permitting these information to be accessible to the clients simultaneously. The instance of these instruments is the antivirus program. Organization security alludes to any action intended to ensure the convenience, uprightness, unwavering quality, and well being of information during their transmission on an organization, Network security manages equipment and programming. The movement can be one of the accompanying enemy of infection and against spyware, firewall, Intrusion avoidance frameworks, and Virtual Private Networks. Web Security is measures and methodology used to ensure information during their transmission over an assortment of interconnected organizations, while data security is about how to forestall assaults, and to recognize assaults on data based frameworks.

IV. CRYPTOGRAPHY GOALS

By utilizing cryptography numerous objectives can be achieved[2]. These objectives can be either completely accomplished simultaneously in one application, or just one of them. These objectives are:

1. Privacy: it is the main objective, that guarantees that no one can comprehend the got message aside from the person who has the interpret key.

2. Verification: it is the way toward demonstrating the character, that guarantees the conveying element is the one that it professed to be. This implies that the client or the framework can demonstrate their own characters to different gatherings who don't have individual information on their personalities.

3. Information Integrity: its guarantees that the got message has not been changed at all from its unique structure. The information may get adjusted by an unapproved element purposefully or accidently. Respectability administration affirms that if information is flawless since it was last made, communicated, or put away by an approved client. This can be accomplished by utilizing hashing at the two sides the sender and the beneficiary to make a one of a kind message condensation and contrast it and the one that got.

4. Non-Repudiation: it is framework used to show that the sender genuinely sent this message, and the message was gotten by the predefined party, so the recipient can't ensure that the message was not sent. For example, when a solicitation is put electronically, a purchaser can't deny the purchase demand, if non-denial organization was enabled in this trade.

5. Access Control: it is the route toward thwarting an unapproved usage of resources. This target controls who can move toward the resources, If one can access, under which constraints and conditions the passage can be occurred, and what is the assent level of a given permission.

V. PROPOSED ALGORITHM

RSA calculation utilized unbalanced keys; one of them for encryption the message, and is known as a public key and another used to unscramble the scrambled message and is known as a private key. The fundamental burden of the RSA calculation is that additional time is taken to play out the encryption cycle. In this investigation, the MATLAB library capacities are executed to accomplish the work. The product encourages us to hold huge prime numbers to create the necessary keys which upgraded the security of communicated data and we expected to be hard for a programmer to meddle with the private data. The calculations are executed effectively on various sizes of messages documents. RSA utilized two prime numbers for encryption and decoding yet as opposed to utilizing two prime numbers we have utilized five prime numbers for private and public key by creating variable n with enormous size. The factorization follows three stages, for example, key age, encryption and unscrambling.

For instance:

Key generation:

Select five prime numbers-p, q, r,s and t

- Calculate n=p*q*r*s*t.
- Calculate phi = (p-1)*(q-1)*(r-1)*(s-1)*(t-1)
- Select an integer e such that 1<e<phi and GCD (e, phi) =1; e and phi are co prime.
- Choose a number relatively prime to phi and call it d.
- Find d such that e*d=1mod phi

Encryption

Cipher text, C= Me mod n

Decryption

Plain text, M= Cd mod n

VI. RSA AND PROPOSED ALGORITHM COMPARISION

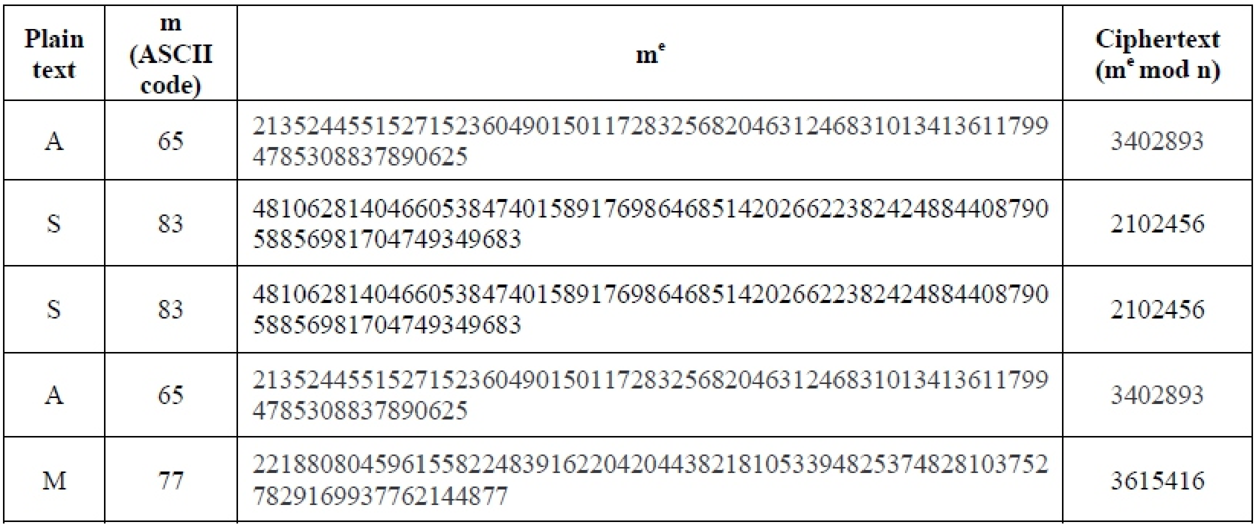
Key generation

Choose p=51 q=43 r=13s=19t=7
Compute N= 3791697
Compute phi= 2721600
Let e=41
Find d such that e*d=1
mod phi d= 132761
Public key (e, n) = (41, 3791697)
Private Key (d, n) = (132761, 3791697)

Encryption

With the help of public key we are able to encrypt the value of plain text. Enter the value of plain text and we get the cipher text.

Suppose the message to be encrypted is ASSAM

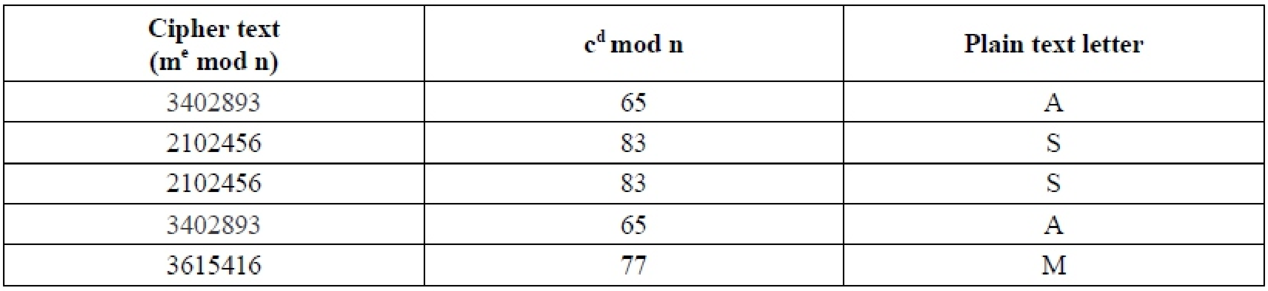


Plain text	m (ASCII code)	m^e	Ciphertext (m^e mod n)
A	65	21352445515271523604901501172832568204631246831013413611799 4785308837890625	3402893
S	83	48106281404660538474015891769864685142026622382424884408790 58856981704749349683	2102456
S	83	48106281404660538474015891769864685142026622382424884408790 58856981704749349683	2102456
A	65	21352445515271523604901501172832568204631246831013413611799 4785308837890625	3402893
M	77	22188080459615582248391622042044382181053394825374828103752 7829169937762144877	3615416

TABLE1: ENCRYPTION PROCESS

Decryption Process:

With the help of the private key the cipher text can be converted to plain text. Compute P=C^d mod n by using private key.

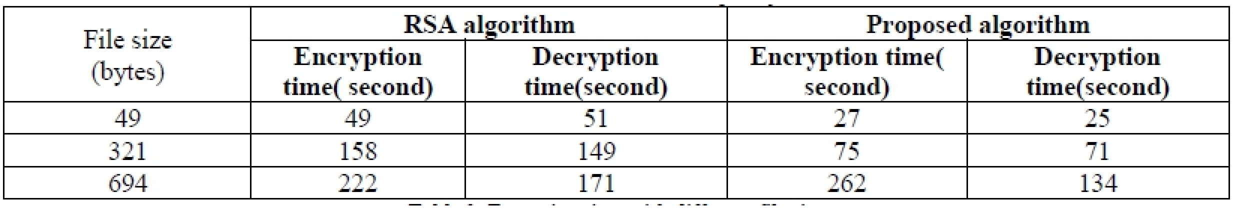


Cipher text (m^e mod n)	c^d mod n	Plain text letter
3402893	65	A
2102456	83	S
2102456	83	S
3402893	65	A
3615416	77	M

TABLE2: DECRYPTION PROCESS

Decrypted value of the cipher text: ASSAM

The following times were recorded while encrypting/decrypting data-



File size (bytes)	RSA algorithm		Proposed algorithm	
	Encryption time(second)	Decryption time(second)	Encryption time(second)	Decryption time(second)
49	49	51	27	25
321	158	149	75	71
694	222	171	262	134

Table 3: Execution time with different file size

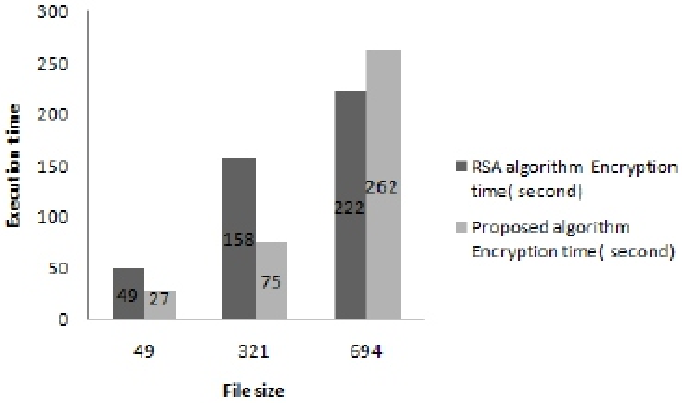


Figure1. Encryption time with different file size

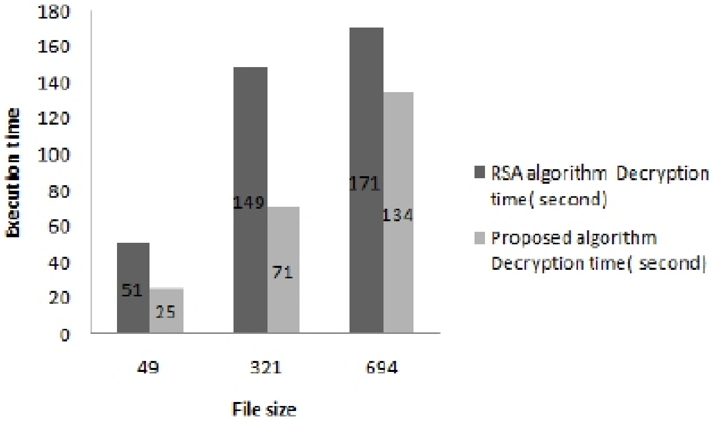


Figure2. Decryption time with different file size

VII. CONCLUSION

At the point when the code text is decoded with the assistance of private key, same plain content has been noticed. Subsequent to examining RSA and altered RSA, it is discovered that the proposed calculation expands the security of the framework as it diminishes the calculation time. This shows that exactness of upgraded RSA cryptographic calculation utilizing dynamic keys is acceptable. Investigation of different encryption calculations has indicated that the strength of the calculation relies upon the length of the key. Key length is straightforwardly relative to security and conversely corresponding to execution. Accordingly hacking time is decreased which show that the time accessible for the programmer has been diminished.

REFERENCE

[1] Meneses F., Fuertes W., José Sancho, Salvador S., Flores D., Aules H., Castro F. Torres J., Miranda A., Nuela D., "RSA Encryption Algorithm Optimization to Improve Performance and Security Level of Network Messages", IJCSNS International Journal of Computer Science and Network Security, VOL.16 No.8, 2016.

[2] Jamgekar R. S., Joshi G.S., "File Encryption and Decryption Using Secure RSA," International Journal of Emerging Science and Engineering (IJESE), ISSN: 2319–6378, Volume-1, Issue-4,2013.

[3] Obaid T. A. S. Khami M. Shehab L. G., "Hiding Secured key in digital media", Int. Jo. Eng. Res. App., ISSN: 2248-9622, Vol. 7, Issue 9, pp.58-63, www.ijera.com,2017

[4] Nisha S., and Farik M.," RSA Public Key Cryptography Algorithm – A Review", International Journal of Scientific & Technology Research Volume 6, Issue 07, ISSN 2277-8616, 2017.

[5] Khyoon, A. I., "Modification on the Algorithm of RSA Cryptography System," Al-Fatih Journal, ISSN: 87521996, Volume: 1 Issue: 24 Pages: 80-89, 2005.

[6] Al-Lehiebe A., " Ciphered Text Hiding in an Image using RSA algorithm", J. Of College of Education for Women vol. 26 (3), 2015.

[7] Cid C., " Cryptanalysis of RSA: A Survey", SANS Institute.Bonde S. Y.; Bhadade U.S., International Conference on Computing, Communication, Control and Automation (ICCUBEA)", DOI: 10.1109/ICCUBEA .8463720, Publisher: IEEE, 2019.

[8] Patel S. R., Shah K., Patel G. R., "Study on Improvements in RSA Algorithm," IJEDR, ISSN: 2321-9939, 2013.

ISSN NO. (Print) : 2320-2106, (Online): 2321-2063

Encryption Algorithms: Review on Application in Various Fields

[1] Dharitri Talukdar, [2] Laba Kr. Thakuria, [3] L. P. Saikia
[1]Research Scholar, Assam down Town University, Guwahati, Assam, India
[2]Deputy Controller of Examination, Assam Down Town University, Guwahati, Assam, India
[3]Professor, Girijananda Chowdhary Institute of Management and Technology, Guwahati, Assam, India
E-mail: [1]dharitritalukdar03@gmail.com,[2]thakurialaba@gmail.com,[3]lp_saikia@yahoo.co.in

ABSTRACT

Due to enormous increase in the usage of internet, today's world is currently flooded with huge volumes of data. Security is one of the vital concerns especially in the current period with an extensive rise in the usage of the internet as most of works are digitally done from sending mail to sharing bank details. So, an effective encryption algorithm is of greater need for achieving an immense amount of privacy. Cryptography is utilized to make sure about completely sent data, to authenticate people and devices, and devices to other devices. They assume a critical part in guaranteeing the classification and validness of interchanges on the Internet and different organizations. This paper is basically centered around various uses of encryption calculations and utilization of cryptography, in actuality.

Keywords - Encryption, Cryptography, Application, Network Security, RSA

I. INTRODUCTION

Cryptography is no longer limited to the military but today we use cryptography in our everyday life hundreds of times a day. From remotely unlocking car with the key fob to using all kinds of devices. This ancient art underpins modern life too. The same is true in computer systems. For example the lock on the website that people are browsing, E-commerce, online banking, online shopping and other emerging things, which greatly enriches and facilitates people‟s lives. However, at the same time, the network information leakage, tampering and counterfeiting, hacking, computer crime, computer virus spread, all these problems have become a major threat to network information security. Information security is increasingly becoming the focus of attention [1]. At present, information security is an important part of national security. To overcome this situation, they often use strong cryptographic keys and algorithms. It‟s about encoding transmission data and transforming them into something unreadable to anyone other than who the information is meant for.

II. LITERATURE REVIEW

Ankit Anand [6] et.al in 2012 concluded that proper interface design and a well implemented device driver are needed to provide the same throughput on application layer as on the hardware layer and we have got the waveform successfully after simulation and also got the hardware design for RSA after synthesis.

In August 2000, NIST selected five algorithms: Mars, RC6, Rijndael, Serpent and Twofish as the final competitors [3]. These algorithms were subject to further analysis prior to the selection of the best algorithm for the AES. Finally, on October 2, 2000, NIST announced that the Rijndael algorithm was the winner. Field Programmable Gate Arrays (FPGAs) are hardware devices whose function is not fixed which can be programmed in system. Advanced Encryption Algorithm includes efficiency testing of both hardware and software implementations of candidate algorithms. Reprogrammable devices such a s field-programmable gate arrays (FPGAs) are highly attractive options for hardware implementations of encryption algorithms, as they provide physical security, and potentially much higher performance than software solutions. Thambiraja [7] et al showed that AES consumes highest processing power among DES, 3DES, BLOWFISH. AES is better than RC4 for smaller packets also it is better for live video streaming transmission compared to RC4 and XOR. Time taken by RSA is much higher than that of AES and DES. Memory usage of RSA is high compared to AES, DES. Output byte in RSA is less as compared to AES and DES.RC4 is fast and energy efficient than AES for larger packets. Time for encryption and decryption almost remains constant for RC4 if key size is increased and less time is required to encrypt as compared to AES, DES, and 3DES.

III. WEB SECURITY

Web security or cyber security basically means a system of protection measures and protocols that can protect website or web application from being hacked or entered by unauthorized personnel. This integral division of information security is vital to the protection of websites, web applications, and web services. Unfortunately, cybercrime happens every day, and great web security measures are needed to protect websites and web applications from becoming compromised. There are a lot of factors that go into web security and web protection. Any website or application that is secure is surely backed by different types of checkpoints and techniques for keeping it safe.

There are a variety of security standards that must be followed at all times, and these standards are implemented and highlighted by the OWASP. Most experienced web developers from top cyber security companies will follow the standards of the OWASP as well as keep a close eye on the Web Hacking Incident Database to see when, how, and why different people are hacking different websites and services. Essential steps in protecting web apps from attacks include applying up-to-date encryption, setting proper authentication, continuously patching discovered vulnerabilities, avoiding data theft by having secure software development practices. The reality is that clever attackers may be competent enough to find flaws even in a fairly robust secured environment, and so a holistic security strategy is advised. There are different types of technologies available for maintaining the best security standards. Some popular technical solutions for testing, building, and preventing threats include:

- Black box testing tools
- Fuzzing tools
- White box testing tools
- Web application firewalls (WAF)
- Security or vulnerability scanners
- Password cracking tools

IV. APPLICATIONS OF ENCRYPTION ALGORITHMS IN DIFFERENT FIELDS

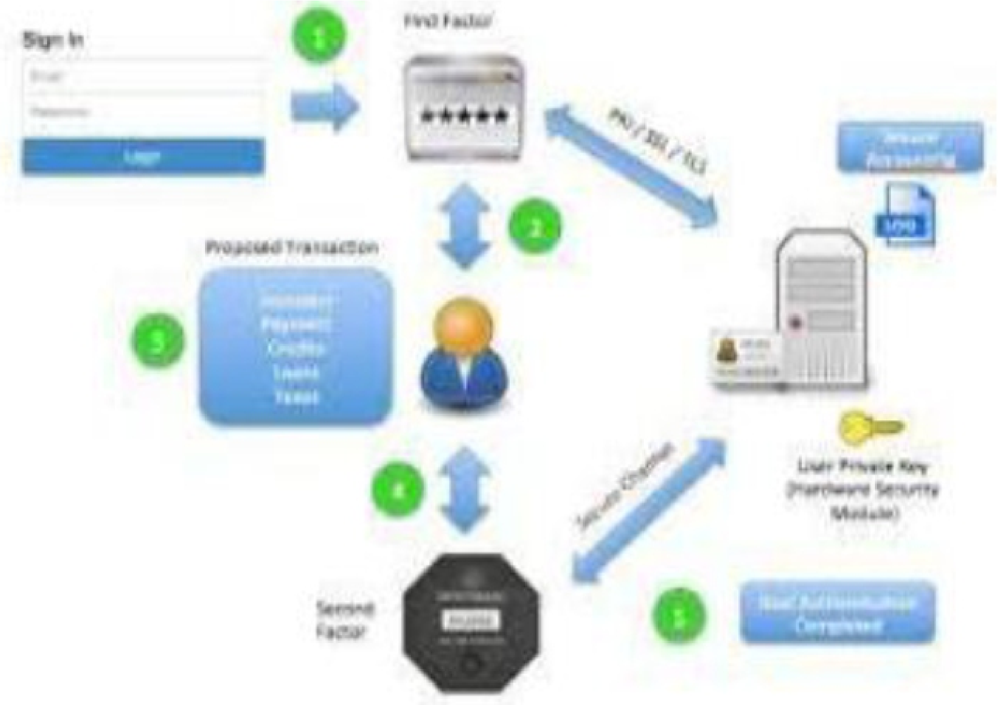
Cryptography originated about 4000 years ago, and the world of cryptography has evolved a lot since then and is omnipresent in our lives without most of us realizing it. RSA is used mostly in hybrid encryption schemes and digital signatures. RSA is also used regularly in web browsers, chat applications, email, VPNs, and any other types of communications that require securely sending data to servers or people. Here we will discuss about the application and use of cryptography in practical field.Computer applications, programming, and equipment all incorporate encryption to achieve targets that clients esteem. A solitary PC or cell phone today, for example, generally sends encryption in numerous various ways, remembering for the equipment, the firmware that interfaces the equipment and the working framework, and a huge part of the product those sudden spikes in demand for the gadget.

The inescapability of encryption is pertinent to public discussions about extraordinary access, in light of the fact that lone certain employments of cryptography in a PC or cell phone empower encryption of clients' information of expected interest to law implementation or insight offices. Hence an order for excellent access would need to be focused to explicit employments of cryptography where the points of interest change as indicated by the gadget. This part gives some exceptionally disentangled instances of a portion of these applications and the manners in which that they rely upon encryption; the emphasis is on giving a feeling of the function of encryption as opposed to full subtleties of its execution.

• Card Payment Security Using RSA

The RSA algorithm is public key encryption algorithm which is a widely accepted and implemented by public. The use of RSA in card payment system makes the process more secure [4]. Now the bank transactions can be done securely without worrying about attacker getting access to the database as the data will be in encrypted form.

• Authentication/Digital Signatures



Authentication is any cycle through which one demonstrates and checks certain data. Now and then one might need to check the source of a report, the character of the sender, the time and date an archive was sent as well as marked, the personality of a PC or client, etc. An advanced mark is a cryptographic methods through which a considerable lot of these might be checked. The computerized mark of a record is a snippet of data dependent on both the archive and the underwriter's private key. It is regularly made using a hash work and a private marking capacity (calculations that make encypyted characters containing explicit data about a record and its private keys).

• Role of RSA in E-commerce

E-business is the most popular business these days. They manage a ton of delicate information of their clients. Security has become a tremendously important. Innovation has unquestionably been progressed however hazard has expanded too with the expansion of digital violations. Here comes the need of cryptography to provide data security for such e-businesses. The RSA algorithm is ordinarily utilized for making sure about interchanges between internet browsers and online business locales. The explanation behind this is the protection from assault. The association utilizes a safe attachment layer (SSL) authentication, which is made from the general population and private keys. E-trade has introduced another method of doing exchanges everywhere on the world utilizing web. The achievement of internet business relies extraordinarily upon how its data innovation is utilized. There is a developing requirement for innovative answers for universally secure web based business exchange in arrangement by utilizing suitable information security innovation. The innovation arrangement proposed for tackling this security issue is the RSA cryptosystem.

- **Encryption in Whatsapp**

„Whatsapp‟ is currently one of the most popular messaging services in the worlds. It is available for different platforms such as Android, Windows Phone, and iPhone. In the latest version of „Whatsapp,‟ the conversations and calls are "end-to-end" encrypted[3]. When end-to-end encrypted, all messages, photos, videos, voice messages, documents, and calls are secured from falling into the wrong hands that ensures only sender and receiver can read what is sent, and no one in the middle of, not even Whatsapp. This is because all the messages are made sure about with a lock, and as it were the beneficiary and sender have the extraordinary key needed to unlock and read them as every message has its own remarkable lock and key. While exchanging message a session has been established, clients exchange messages that are protected with a Message Key using AES256 in CBC mode for encryption and HMAC-SHA256 for authentication [2]. End-to-end encryption use Noise Pipes with Curve25519, AES-GCM, and SHA256 from the Noise Protocol Framework for long running interactive connections.

- **Encryption in Bank in/Money**

RSA calculation is generally utilized by banks to secure their information, similar to client data and exchange record. In today‟s digital world, banking transactions are mostly done through ATM (Automated Teller Machine) or through electronic transactions. RSA Algorithm is utilized to scramble and decode information in present day PC frameworks and other electronic gadgets. The correspondence security techniques utilized between auto teller machine and bank worker banking monetary tasks, when they communicate information from an Auto Teller Machine (ATM) to bank worker it must send in encoded form so that an unauthorized user cannot access the secure information directly at the time of data communication. Triple DES is an encryption algorithm considered Data Encryption Standard that was first utilized by the U.S. Government in the late 1970's. It is ordinarily utilized in ATM machines (to scramble PINs) and is used in UNIX secret key encryption.

The meaning of electronic cash (likewise called electronic money or advanced money) is a term that is as yet developing. It incorporates exchanges did electronically with a net exchange of assets starting with one gathering then onto the next, which might be either charge or credit and can be either unknown or distinguished.

There are both equipment and programming usage. Mysterious applications don't uncover the character of the client and depend on visually impaired mark plans. Distinguished spending plans uncover the character of the client and depend on more broad types of mark plans. Unknown plans are the electronic simple of money, while recognized plans are the electronic simple of a charge or Mastercard. There are likewise some crossover approaches where installments can be mysterious as for the dealer however not the bank ;or unknown to everybody, but rather detectable (an arrangement of buys can be connected, yet not connected straightforwardly to the high-roller's personality).

Encryption is utilized in electronic cash plans to ensure customary exchange information like record numbers and exchange sums, advanced marks can supplant manually written marks or a charge card approvals, and public-key encryption can give privacy. There are a few frameworks that cover this scope of utilizations, from exchanges impersonating traditional paper exchanges with estimations of a few dollars and up, to different micropayment plots that clump incredibly minimal effort exchanges into sums that will bear the overhead of encryption and clearing the bank.

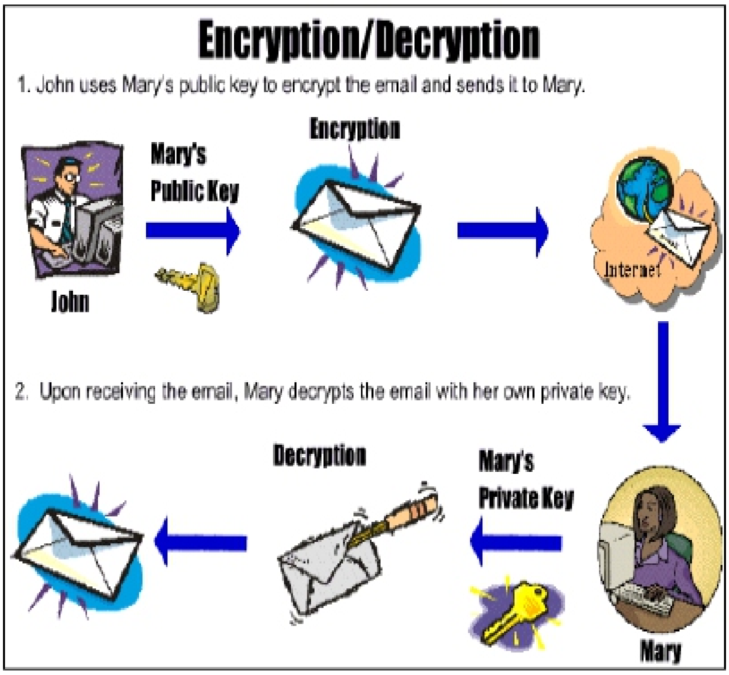
- **RSA in Telecommunications**

RSA calculation is valuable to encode the call information as a worry for protection issues.

- **Encryption/Decryption in email**

Email encryption is a system for ensuring about the substance of messages from anyone outside of the email conversation wanting to get a part's information. In its encoded structure, an email is not, at this point discernible by a human. Just with your private email key can your messages be opened and decoded once again into the first message.

Email encryption works by utilizing something many refer to as open key cryptography. Every individual with an email address has a couple of keys related with that email address, and these keys are needed to encode or decode an email. One of the keys is known as a "public key", and is put away on a keyserver where it is attached to your name and email address and can be gotten to by anybody. The other key is your private key, which isn't shared freely with anybody.


Encryption/Decryption
1. John uses Mary's public key to encrypt the email and sends it to Mary.
Mary's Public Key
Encryption
John
Internet
2. Upon receiving the email, Mary decrypts the email with her own private key.
Decryption
Mary's Private Key
Mary

At the point when an email is sent, it is encoded by a PC utilizing the public key and the substance of the email are transformed into a mind boggling, incomprehensible scramble that is extremely hard to break. This public key can't be utilized to decode the sent message, just to scramble it. Simply the person with the right looking at private key can unscramble the email and read its substance.

There are different sorts of email encryption, however the absolute most regular encryption conventions are:

OpenPGP — such a PGP encryption that uses a decentralized, scattered trust model and encourages well with current web email customers

S/MIME — a kind of encryption that is incorporated into most Apple gadgets and uses a unified power to pick the encryption calculation and key size

Email encryption administrations can be utilized to give encryption in a couple of independent yet related regions:

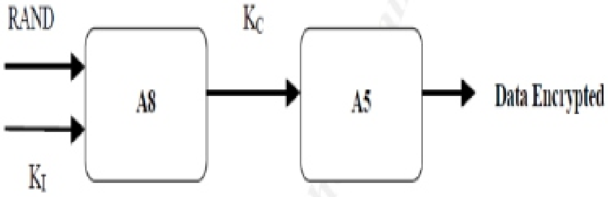
The association between email suppliers can be scrambled, forestalling outside assailants from figuring out how to capture any approaching or active messages as they travel between workers The substance of the email can be encoded, guaranteeing that regardless of whether an email is caught by an assailant, the substance of the email will in any case be totally incoherent Old or documented messages that are now put away inside your email customer ought to likewise be encoded to keep assailants from possibly accessing messages that aren't at present on the way between workers.

- **Encryption in Instagram**

User cooperation with Instagram is likely a scrambled correspondence. At the point when user telephone demands information with instagram it will utilize SSL/TLS over port 443 to scramble demands from Instagram workers and will send information over a similar encoded information stream. This keeps malevolent gatherings from snooping on the discussion among user and instagram.

- **Sim card Authentication**

Confirmation To choose whether or not the SIM may get to the organization, the SIM should be verified. An arbitrary number is produced by the administrator, and is shipped off the cell phone. Along with the mystery key Ki, this irregular number goes through the A3 calculation (it is this Ki that as of late has been undermined). The yield of this estimation is sent back to the administrator, where the yield is contrasted and the figuring that the administrator has executed himself (the administrator has the mystery keys for all SIM cards the administrator has circulated).



Encryption This part is the part that has been broken. So, the administrator creates an irregular number (once more), and sends it to the cell phone. Along with the mystery key Ki, this irregular number goes through the A8 calculation, and produces a meeting key KC. This KC is utilized, in mix with the A5 calculation to encode/decode the information.

V. CONCLUSION

This paper examines various utilizations of encryptions calculations and utilization of cryptography, in actuality. In Data correspondence, encryption calculation assumes a significant job. RSA is an asymmetric encryption algorithm used to encrypt and decrypt data in modern computer systems and other electronic devices. However RSA algorithm used in banking, ecommerce, telecommunications and many other transactions that deal with a lot of sensitive data is used as RSA's security lies in the fact that it is hard to reason what is mystery given what is public.

REFERENCE

[1] Zhou Y.,ZhouG., WeiQ., YuanX., ChengL. (2010). Design of Drone Data Generate System Based on Data Encryption Technology. Informatization Research, 36 (10), 40-42.

[2] "Whatsapp Encryption Overview Technical white paper", December 19, 2017 Originally published April 5, 2016.

[3] https://indianexpress.com/article/technology/social/five-upcoming-whatsapp-features-6448040.

[4] https://nevonprojects.com/card-payment-security-using-rsa

[5] Hoang Trang and Nguyen Van LoiHoChiMinh City, VietNam- "An efficient FPGA implementation of the Advanced Encryption Standard algorithm" 978-1-4673- 0309-5/12/ ©2012 IEEE.

[6] Ankit Anand and Pushkar Praveen, "Implementation of RSA Algorithm on FPGA", Centre for Development of Advanced Computing, (CDAC) Noida, India, ISSN (Online) : 2278-0181 Volume 01, Issue 05 (July 2012)

[7] E. Thambiraja, G. Ramesh and Dr. R. Umarani, "A Survey on Various Most Common Encryption Techniques",International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, July 2012 ISSN: 2277 128X.

ISSN NO. (Print) : 2320-2106, (Online): 2321-2063

Optimization of Multivariable System Control using Neural Network-based Control

[1] Hamid Alshareefi, [2] Ciprian Lupu, [3] Laith Ismail, [4] Lich Duc Luu
[1,2,3,4]Faculty of Automatic Control and Computers, Politehnica University of Bucharest, Bucharest, Romania
E-mail: [1]hamedgep@yahoo.com, [2]ciprian.lupu@acse.pub.ro, [3]laith_ismail@turath.edu.iq, [4]lanlich@gmail.com

ABSTRACT

This paper shows the improvement of controller designing for a multivariable system, through the implementing and testing in real-time the classical methods for controlling the nonlinear multi-input multi-output system (MIMO), where the decentralized strategy, the proportional-integral-derivative controller (PID) used and the advanced method where the dynamic decoupling approach implemented and tested in real-time and the proposed strategy by using intelligent controller where the neural network-based internal model controller (DIC) and internal model controller (IMC) are concisely described and tested in real-time. A short study of the advantages and disadvantages of the proposed strategy compared with the classical strategies. The whole software algorithms were designed and tested in real-time by NI LabVIEW software.

Keywords - Multivariable System, Decentralized Strategy, Dynamic Decoupling, Neural Network, LabVIEW.

I. INTRODUCTION

Most industrial processes are in sense of multivariable systems like chemical, aircraft, robots, and other applications. It's a common industrial practice to reduce a multivariable control problem to the SISO control approach with minimal interaction effect between system loops [1], [2]. Many valuable methods, strategies, and solutions were presented for solving this problem, some of them were based on decentralized control strategy others went towards static or dynamic decoupling strategy. The proposed solution of this paper depends on artificial intelligence where two types of neural controllers are designed based on the neural network theory. Direct inverse control method (DIC) and internal model control (IMC) [3]. All the strategies (classical and proposed) are implemented and tested in real-time by NI LabVIEW software starting with the decentralized control strategy which is less efficient and dynamic decoupling strategy which is a more powerful strategy and finally with the proposed and more optimized strategy by using a neural controller and showing the comparison of the real-time output response for each strategy.

II. MULTIVARIABLE CLASSICAL CONTROL STRATEGY

2.1. Decentralized control strategy

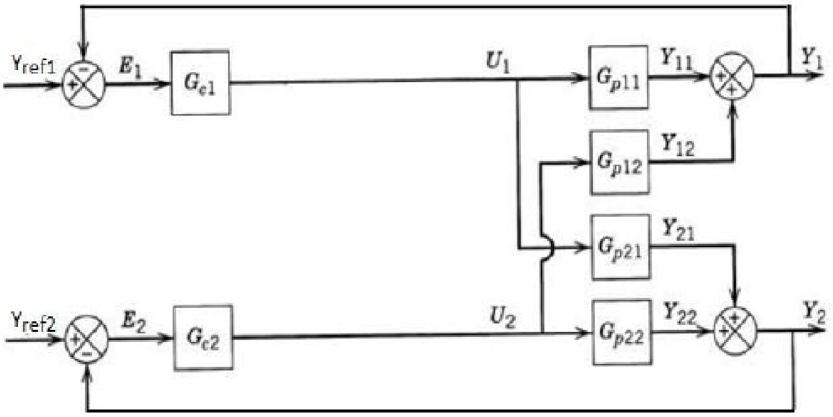


Fig.1. Decentralized control structure

The decentralized controllers are widely used because of their simplicity in hardware, design, and tuning simplicity, the main idea behind it is to deal with MIMO system as multi SISO systems totally independent as shown in Fig. 1. Each

Controller is robust enough to reject the interaction or the disturbance comes from the parallel SISO system

2.1. Dynamic decoupling control strategy

In this strategy, additional decoupling blocks are generally introduced between the multivariable process and the N independent control algorithms; these blocks represent the ratio of the interaction transfer functions between loops as shown in Fig. 2 and eq. (1). The main function of these decoupling blocks is to cancel the negative interference effect of the parallel loops

$$D21 = -\frac{Gp\,21}{Gp\,22} \qquad (1)$$

$$D12 = -\frac{Gp\,12}{Gp\,11}$$

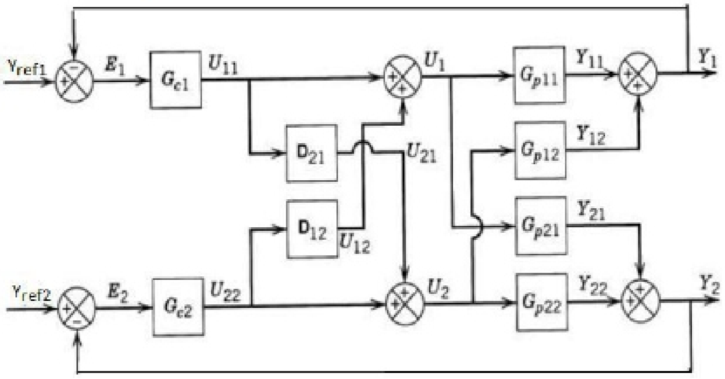


Fig.2. Dynamic decoupling control structure

There are some issues that have to be handled when working with the classical strategies as summarized below

1. Eliminating unworkable variable pairing of the parallel loops. The pairing can be done with relative gain array (RGA) matrix or Niederlinski indices (NI).
2. Finding the best pairing from the remaining sets.
3. Tune all controllers using an efficient methodology.

III. ARTIFICIAL NEURAL NETWORK-BASED CONTROL STRATEGIES

Artificial neural network (ANN) is a reliable and widely used tool when handling problems including the prediction of variables at the present age. Details of the ANN application can be found in the literature [4] [5]. The main feature of ANN is its ability to estimate the dynamic model of a random function that learns from data input into the network. The first important issue is the choice of the model based on data representation and application. The other issue that is included for training is a robust analysis for the model, the cost function and the learning algorithm must be appropriately selected, so that the final result of ANN can be robust. The neural network has been widely used in a wide range of applications including identification, control, and prediction. As for today feedforward neural network (FANN), architecture is the widely used neural network architecture. It has a global approximation model for a multi-input multi-output function for fitting a low-order polynomial through a set of data. Various collections of learning and network algorithms are available [6, 7]. Fig. 3 and eq. (2) show the mathematical form describing the neural network formula and the feedforward algorithm.

$$\mathrm{Yn} = \mathrm{F1}\left(\sum_{l=1,j=1}^{k,m} \mathrm{WOlj} * \mathrm{F0}\left(\sum_{j=1,l=1}^{n,k} \mathrm{WilXi} + \mathrm{Bk}\right) + \mathrm{Bom}\right) \qquad (2)$$

Where $Y_n=[y_{n1}..y_{nm}]$ represent the outputs of the neural networks, $WO=[wo_{11}..wo_{km}]$ the weights of output nodes neurons, $W=[w_{11}..w_{nk}]$ the hidden layer nodes neurons, $X=[x_1..x_n]$ the inputs of the network, $B=[b_1..b_k]$ the bias of hidden layer nodes, $BO=[b_{o1}..b_{om}]$ the bias of output layer nodes, F_1, F represent the activation functions which could be sigmoid, tangent sigmoid, Gaussian or other activation function. In this paper, the sigmoid function is used eq. (3).

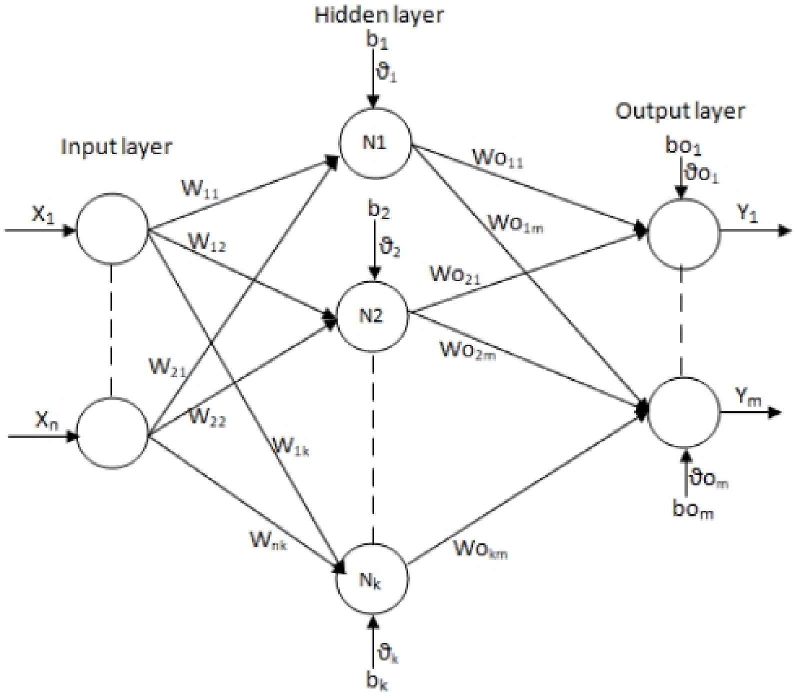


Fig.3. General neural network architectures

$$\mathrm{f(x)} = \frac{1}{1 + e^{-x}} \qquad (3)$$

For the back propagation and learning algorithm, gradient descent is widely used for tuning and optimizing the weights of all neurons which makes the cost function converge to zero eq. (4)

$$\mathrm{j(k)} = \frac{1}{2}\left(\mathrm{e1}^2 + \cdots + \mathrm{ek}^2\right) \qquad (4)$$
$$\mathrm{ek} = \mathrm{yk} - \mathrm{yrefk}$$

Where j(k) is the cost function, $(e_1 \ldots e_k)$ the error of plant outputs. The weights learning is by driving the cost function to all weights in hidden and output node layers eq. (5).

$$\mathrm{W} = \mathrm{W} + \alpha * \frac{\partial \mathrm{J}}{\partial \mathrm{W}} \qquad (5)$$
$$\mathrm{W0} = \mathrm{W0} + \alpha * \frac{\partial \mathrm{J}}{\partial \mathrm{W0}}$$

And the same method for learning the weights of the input bias for both hidden and output layers eq. (6

$$\vartheta = \vartheta + \alpha * \frac{\partial \mathrm{J}}{\partial \vartheta} \qquad (6)$$
$$\vartheta\mathrm{o} = \vartheta\mathrm{o} + \alpha * \frac{\partial \mathrm{J}}{\partial \vartheta\mathrm{o}}$$

There are two types of control strategies in neural network-based control

3.1. Direct inverse control method (DIC).

In this strategy, the neural network inverse model acts as a controller. The output will predict the system input, while the desired reference represents the output which is fed to the network with the past plant input.

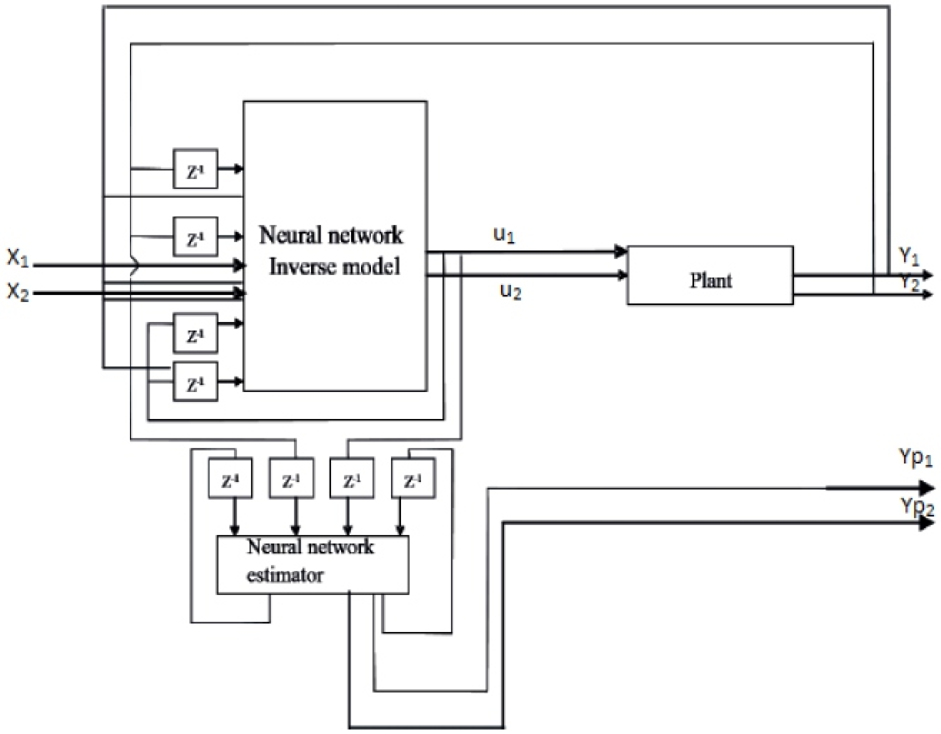


Fig. 4. Neural network-based direct inverse model control (DIC).

In this case, the proper control parameters for the desired reference will be predicted based on its input. As shown in Fig. 4, the inverse model was then used in the control by companied it with the controlled system. This method depends on the accuracy of the inverse model.

3.2. Internal model control (IMC)

IMC Neural network-based strategy approaching in both inverse and forward model control structure. The dynamic forward model of the plant is placed in parallel within the system. This is important to avoid the mismatches of the model during implementation [8]. Furthermore, the inverse model could also be used as a controller. In this strategy, the error between the plant output and the neural network output is then subtracted from the reference before being supplied into the inverse model, as shown in Fig. 5. With this detection feature, the internal model-based controller can be used to move forward the controlled parameter to the desired set point even when disturbances and noise are present. The optimum performance for controller performance is the IMC method. The error produced by the plant model could be minimized and optimized by the error produced by the neural network model [8].

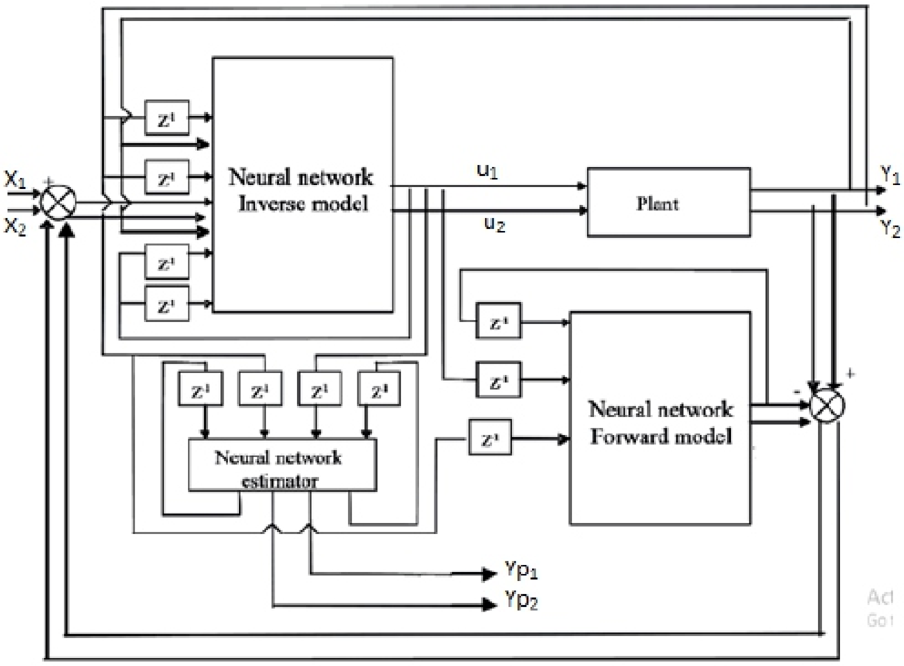


Fig. 5. Neural network-based internal model controller (IMC).

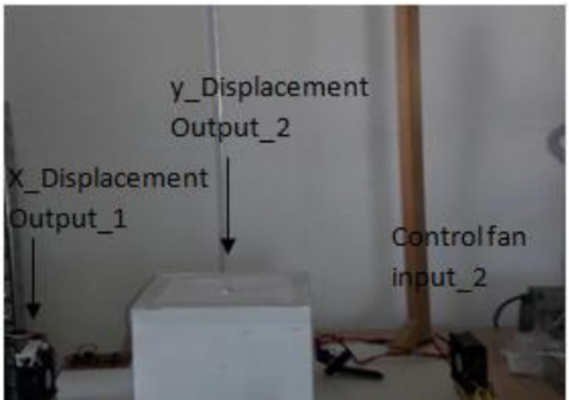


Fig.6. Two-direction position control system

IV. REAL-TIME RESULTS

4.1. Real-time testing of decentralized strategy

All the control strategies were implemented and tested on a laboratory-made system consist of a cubic box hanged vertically like a pendulum and contain four fans two of them with fixed speed to give the system a nonlinearity and the other two fans are the controlled fans which represent the input of the system. On the opposite side of each control fan, there is a displacement sensor represent the outputs of the system. The system is 2 inputs and 2 outputs as shown in Fig. 6 the target is to control the position of the cubic box in the x and y direction through the speed control of the controlled fans. NI USB-6008 interface card used for the data acquisition and all the algorithms are written by LabVIEW software. The first strategy tested is the decentralized strategy. For solving the problem of designing a robust PID controller for each independent loop of the multivariable system, the identification of both system transfer function should be considered by applying a pseudo-random binary signal (PRBS) for the first input with applying a step value for the other input and acquisition the data from the first output. The same procedure to find the transfer function of the second loop by applying the PRBS input to the second input with keeping a fixed value for the first input. For the identification of the dynamic model for each loop, two transfer functions have been identified using the WINPIM as in eq. (7), (8)

$$G11 = \frac{0.04493S + 0\ .03326}{S^2 +\ 0.475S + 0.289} \tag{7}$$

$$G22 = \frac{0.029S + 0\ .0282}{S^2 +\ 0.062S + 0.24} \tag{8}$$

And by using the WINREG software to find the suitable PID controller and test the whole system with two random references as shown in Fig. (7). From the Output response for both references it's obvious that still, the interacted loop affects each other which degrades the final output response for each output.

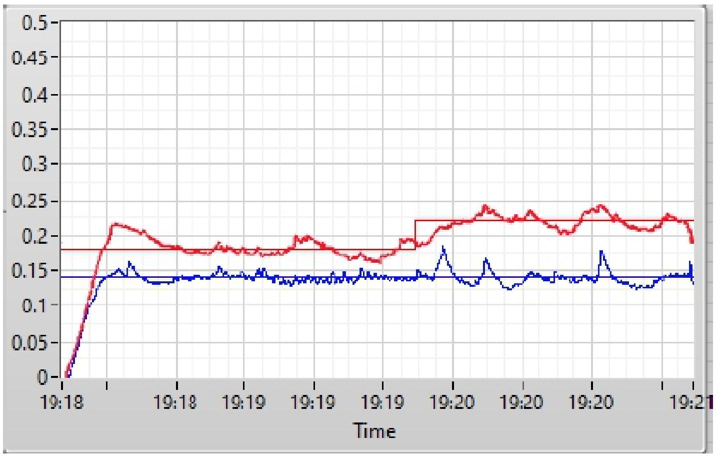


Fig.7. Real-time output response using a decentralized control strategy

4.2. Real-time testing of dynamic decoupling strategy

From the data acquisition in the identification stage of a decentralized strategy, it's possible to identify the transfer function of the interaction effect of the first input on the second output to find G21 and the second input on the first output to find G12, eq. (9) and (10)

$$G21 = \frac{0.00226S + 0\,.0004}{S^2 + 0.206S + 0.0101} \qquad (9)$$

$$G12 = \frac{0.0084S + 0\,.018}{S^2 + 1.05S + 0.305} \qquad (10)$$

According to eq. (1) the dynamic decoupling will be

$$D21 = -\frac{(0.00226S + 0\,.0004) * (S^2 + 0.062S + 0.24)}{(S^2 + 0.206S + 0.0101) * (0.029S + 0\,.0282)} \quad (11)$$

$$D12 = -\frac{(0.0084S + 0\,.018) * (S^2 + 0.475S + 0.289)}{(S^2 + 1.05S + 0.305) * (0.04493S + 0\,.03326)} \quad (12)$$

And by testing the same system with dynamic decouplers it's clear to see the improvement in output response and the lowest interaction between loops output but still, there is small interaction between loops as shown in Fig. (8).

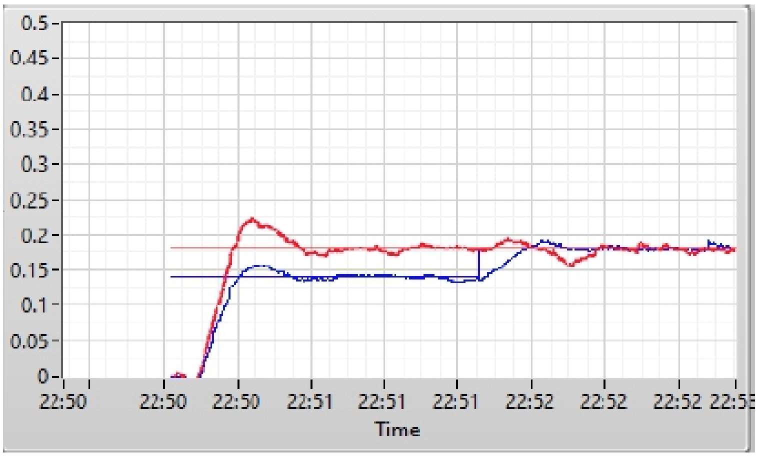


Fig.8. Real-time output response using a dynamic decupling control strategy

4.3. Real-time testing of the neural controller

For a real-time test, has been using the strategy of direct inverse control where the control input to the plant will be according to the eq. (13).

$$U = f^{-1}(Yp(k+1), Yp(k), Yp(k-1) \ldots ,$$
$$ypk - m, Uk, Uk{-}1 \ldots, Uk{-}n \qquad (13)$$

Where Y_p=[y_{p1}.., y_{pm}] represents the predicted outputs of a neural estimator and U=[u_1.., u_n] represents the control commands out from (DIC) block. Furthermore, the more stable controller has been using the learning rates of the Back propagation algorithm as an adapted factor, not a fixed value which insure fast and guaranteed convergence to the target reference and more stable system. Brief driving of adapting learning rate according to Lyapunov function in [9]. Fig. 9 shows the improvement of the output response of the MIMO system with two inputs and two outputs using Neural network-based direct inverse control (DIC).

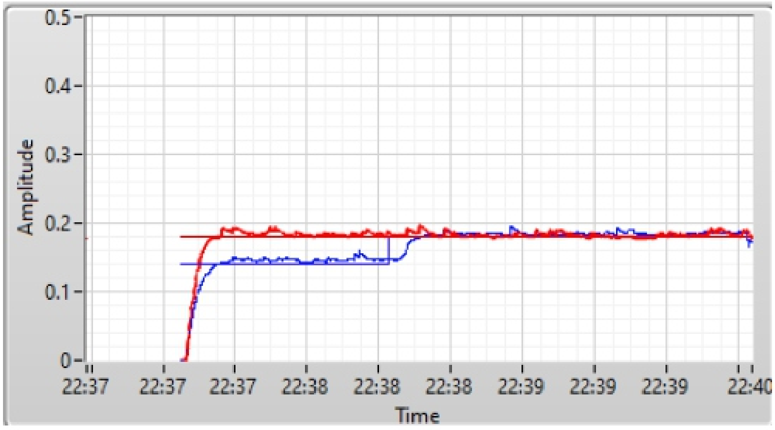


Fig.1. Real-time output response Neural network-based direct inverse control (DIC)

4.3. Advantage and disadvantage of the proposed strategy

Advantages of a neural network-based control strategy for multivariable system summarized below

- The neural controller is a type of nonlinear, multivariable, model-based control. The difference is that, instead of creating the nonlinear process model with explicit equations, the neural controller builds its own process model based on the actual operation which makes the neural controller has the ability of prediction.
- Online training leads to the real-time optimizing of the process.
- Fast converges to the references due to the adapting of the learning rate
- Avoiding the difficulties and mismatching of the dynamic model identification
- Disadvantages of a neural network-based control strategy
- A neural controller is an empirical, rather than a theoretical model, this leads to difficult achievement a specific characteristics and performance requirements.
- Changing in sample time may lead to instability.
- According to the missing of the mathematical model lead to the Missing of the ability to determine the unwanted frequencies

V. CONCLUSION

Multi variables system is widely spread in industrial fields and automatic control applications. In most cases, the real process is very complicated dynamically and it's difficult or less accurate to represent them mathematically. In this paper, we showed a concise description and real-time comparative study of controller design for multivariable systems between the classical strategy represented by decentralized control strategy and dynamic decoupling control with the proposed strategy which is the neural network-based control strategy. Some advantages and disadvantages are mentioned for a fair comparison between strategies.

REFERENCE

[1] I. D. Landau, R. Lozano and M. M'Saad, Adaptive Control, Springer Verlag, London, 1997

[2] C. Lupu, D. Popescu, A. Udrea, C. Dimon, Solutions for Nonlinear Multivariable Processes Control, WSEAS Transactions on Systems and Control,Issues 6, Vol. 3, June 2008, pp. 597-606.

[3] Nasser Mohamed Ramli (December 20th 2017). Advanced Process Control, Advanced Applications for Artificial Neural Networks, Adel El-Shahat, IntechOpen, DOI: 10.5772/intechopen.70704

[4] Hussain MA. Review of the application of neural networks in chemical process control—Simulation and online implementation. Artificial Intelligence in Engineering. 1999; 13:55-68. DOI: S0954-1810(98)00011-9

[5] Ghasem NM, Sata SA, Hussain MA. Temperature control of a bench scale batch polymerization reactor for polystyrene production. Chemical Engineering Technology. 2007; 30: 1193-1202

[6] Norgaad M, Poulsen N, Hansen L. Neural Networks for Modeling and Control of Dynamic Systems. London: Springer Verlag; 2000. DOI: 10.1002/rnc.585/pdf.

[7] Haykin S. Neural Network—A Comprehensive Foundation. New Jersey: Prentice Hall Inc; 1999. DOI: 10.1017/S0269888998004019

[8] Ng CW, Hussain MA. Hybrid neural network prior knolwledge model in temperature control of a semi batch polymerization process. Chemical Engineering and Processing. 2004;43:559-570. DOI: 10.1016/S0255-2701(03)00109-0

[9] T. Korkobi, M. Djemel, and M. Chtourou, "Stability analysis of neural networks-based system identification,"Modelling and Simulation in Engineering, vol. 2008, Article ID 343940, 8 pages, 2008. Kittisupakorn P, Thitiyasook P, Hussain MA, Daosud W. Neural network based model predictive for a steel pickling process. Journal of Process Control. 2009; 19:579-590. DOI: 10.1016/j.jprocont.2008.09.003

[10] Ng CW, Hussain MA. Hybrid neural network prior knolwledge model in temperature control of a semi batch polymerization process. Chemical Engineering and Processing. 2004; 43:559-570. DOI: 10.1016/S0255-2701(03)00109-0

Instructions for Authors

Essentials for Publishing in this Journal

1 Submitted articles should not have been previously published or be currently under consideration for publication elsewhere.

2 Conference papers may only be submitted if the paper has been completely re-written (taken to mean more than 50%) and the author has cleared any necessary permission with the copyright owner if it has been previously copyrighted.

3 All our articles are refereed through a double-blind process.

4 All authors must declare they have read and agreed to the content of the submitted article and must sign a declaration correspond to the originality of the article.

Submission Process

All articles for this journal must be submitted using our online submissions system. http://enrichedpub.com/ . Please use the Submit Your Article link in the Author Service area.

Manuscript Guidelines

The instructions to authors about the article preparation for publication in the Manuscripts are submitted online, through the e-Ur (Electronic editing) system, developed by **Enriched Publications Pvt. Ltd**. The article should contain the abstract with keywords, introduction, body, conclusion, references and the summary in English language (without heading and subheading enumeration). The article length should not exceed 16 pages of A4 paper format.

Title

The title should be informative. It is in both Journal's and author's best interest to use terms suitable. For indexing and word search. If there are no such terms in the title, the author is strongly advised to add a subtitle. The title should be given in English as well. The titles precede the abstract and the summary in an appropriate language.

Letterhead Title

The letterhead title is given at a top of each page for easier identification of article copies in an Electronic form in particular. It contains the author's surname and first name initial .article title, journal title and collation (year, volume, and issue, first and last page). The journal and article titles can be given in a shortened form.

Author's Name

Full name(s) of author(s) should be used. It is advisable to give the middle initial. Names are given in their original form.

Contact Details

The postal address or the e-mail address of the author (usually of the first one if there are more Authors) is given in the footnote at the bottom of the first page.

Type of Articles

Classification of articles is a duty of the editorial staff and is of special importance. Referees and the members of the editorial staff, or section editors, can propose a category, but the editor-in-chief has the sole responsibility for their classification. Journal articles are classified as follows:

Scientific articles:

1. Original scientific paper (giving the previously unpublished results of the author's own research based on management methods).

2. Survey paper (giving an original, detailed and critical view of a research problem or an area to which the author has made a contribution visible through his self-citation);

3. Short or preliminary communication (original management paper of full format but of a smaller extent or of a preliminary character);

4. Scientific critique or forum (discussion on a particular scientific topic, based exclusively on management argumentation) and commentaries. Exceptionally, in particular areas, a scientific paper in the Journal can be in a form of a monograph or a critical edition of scientific data (historical, archival, lexicographic, bibliographic, data survey, etc.) which were unknown or hardly accessible for scientific research.

Professional articles:

1. Professional paper (contribution offering experience useful for improvement of professional practice but not necessarily based on scientific methods);
2. Informative contribution (editorial, commentary, etc.);
3. Review (of a book, software, case study, scientific event, etc.)

Language

The article should be in English. The grammar and style of the article should be of good quality. The systematized text should be without abbreviations (except standard ones). All measurements must be in SI units. The sequence of formulae is denoted in Arabic numerals in parentheses on the right-hand side.

Abstract and Summary

An abstract is a concise informative presentation of the article content for fast and accurate Evaluation of its relevance. It is both in the Editorial Office's and the author's best interest for an abstract to contain terms often used for indexing and article search. The abstract describes the purpose of the study and the methods, outlines the findings and state the conclusions. A 100- to 250-Word abstract should be placed between the title and the keywords with the body text to follow. Besides an abstract are advised to have a summary in English, at the end of the article, after the Reference list. The summary should be structured and long up to 1/10 of the article length (it is more extensive than the abstract).

Keywords

Keywords are terms or phrases showing adequately the article content for indexing and search purposes. They should be allocated heaving in mind widely accepted international sources (index, dictionary or thesaurus), such as the Web of Science keyword list for science in general. The higher their usage frequency is the better. Up to 10 keywords immediately follow the abstract and the summary, in respective languages.

Acknowledgements

The name and the number of the project or programmed within which the article was realized is given in a separate note at the bottom of the first page together with the name of the institution which financially supported the project or programmed.

Tables and Illustrations

All the captions should be in the original language as well as in English, together with the texts in illustrations if possible. Tables are typed in the same style as the text and are denoted by numerals at the top. Photographs and drawings, placed appropriately in the text, should be clear, precise and suitable for reproduction. Drawings should be created in Word or Corel.

Citation in the Text

Citation in the text must be uniform. When citing references in the text, use the reference number set in square brackets from the Reference list at the end of the article.

Footnotes

Footnotes are given at the bottom of the page with the text they refer to. They can contain less relevant details, additional explanations or used sources (e.g. scientific material, manuals). They cannot replace the cited literature.

The article should be accompanied with a cover letter with the information about the author(s): surname, middle initial, first name, and citizen personal number, rank, title, e-mail address, and affiliation address, home address including municipality, phone number in the office and at home (or a mobile phone number). The cover letter should state the type of the article and tell which illustrations are original and which are not.

Address of the Editorial Office:

Enriched Publications Pvt. Ltd.
S-9,IInd FLOOR, MLU POCKET,
MANISH ABHINAV PLAZA-II, ABOVE FEDERAL BANK,
PLOT NO-5, SECTOR -5, DWARKA, NEW DELHI, INDIA-110075,
PHONE: - + (91)-(11)-45525005