Applications and Usage of Visual Cryptography: A Review

Anjney Pandey[1], **Subhranil Som**[2]

[1,2]Amity Institute of Information Technology, Amity University Uttar Pradesh, Noida, UP, India
[1]anjneypandey1@gmail.com, [2]ssom@amity.edu

Abstract: **Visual cryptography is a cryptographic technique which allows visual information to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer. In this paper, we intend to study the different application areas of Visual Cryptography. Visual Cryptography is a wide area of research used in data hiding, securing images, color imaging, multimedia and other such fields. Visual Cryptography comes in the field of data hiding used in cybercrime, file formats etc. This paper focuses on the application areas of visual cryptography from four different research papers/journals which talk about the most important application areas of visual cryptography.**

Keywords: **visual cryptography, encrypted, data hiding, multimedia, color imaging, cybercrime**

I. INTRODUCTION

Visual Cryptography is a cryptographic technique which allows visual information to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer. In today's computer generation, data security, hiding and all such activities have become probably the most important aspect for most organizations. These organizations spend millions of their currency to just secure their data. This urgency has risen due to increase in cyber theft/ crime. The technology has grown so much that criminals have found multiple ways to perform cybercrime to which the concerned authorities have either less or not sufficient answer to counter. Hence, the method of Cryptography provides the above answers. One of the most majorparts of cryptography is Visual cryptography. It has many usage & application areas, mostly using its internal technique called encryption. Some of those application areas are talked about in this research paper.Visual cryptography is used specifically in the areas of Biometric security, Watermarking, Remote electronic voting, Bank customer identification etc. This research paper contains 4 sections. Section 2 talks about the related work and applications in the field of Visual Cryptography. Section 3 gives the Conclusion of the paper followed by References.

II. RELATED WORK

2.1 Rijndael and RC6 Block Ciphers

Information in different forms such as text, image, multimedia etc is an important tool in today's day-to-day life. Thus,arise the need to protect this information/data from outside interference which can create a threat at a large scale in many cases. In [2], the authors proposed two very efficient techniques to encrypt images with few images using Rijndael and RC6 Block Ciphers in Electronic Code Block (ECB) Mode using pre-processing. Pre-processing enables the algorithms to prevent patterns to emerge in the images before encryption.

Rijndael: The Rijndael block cipher is an iterated block cipher using variable block and key size[2]. It is the only encryption mode using parallel processing. The block cipher algorithm provides mapping of plain text block to cipher text block and consequently, from cipher text block to plain text block using cipher key. Rijndael supports all combinations of block and key sizes of multiple of 32 bits with minimum of 128 bits and maximum of 256 bits.

RC6: The RC6 block cipher depends mainly on four working registers, each of 32 bits. It is a key having variable parameters such as key and block size, number of rounds. RC6 encrypted algorithm is designated as: -RC6 (w,r,b) where w is the word size, r is the number of rounds, b is the number of bytes.

2.1.1Study of Rijndael and RC6 with some resultsVisual Encryption

In [2], the research was based on a medical image with black area and CS logo with white area.

Figure-1 shows the medical image of a brain with black area to be used for encryption.

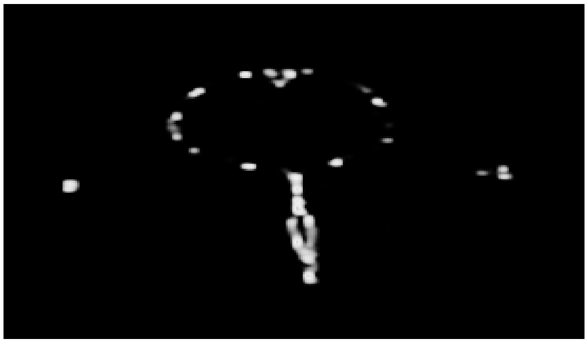


Fig. 1. Medical image of a brain with black area [2]

Figure - 2 is an image consisting of two letters C & S with white area to be used for encryption.

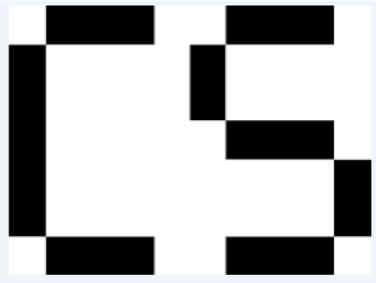


Fig. 2. CS logo with white area [2]

Through the experiments, it was inevitable that Rijndael and RC6 block cipher algorithms work efficiently in ECB Mode using pre- processing. Figure-3 &Figure-4 show the results of the above for both images.

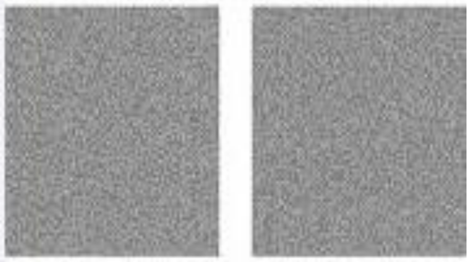


Fig. 3. Encrypted medical images with Rijndael and RC6algorithms in ECB mode using pre- processing [2]

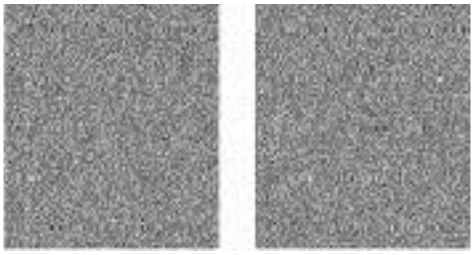


Fig. 4. Encrypted CS logo with Rijndael and RC6 algorithms in ECB mode using pre- processing [2]

Irregularity of Deviation

It calculates the quality of an image through encryption by finding the minimal deviation in comparison to ideal encryption.[2]

Irregular deviation DI is as follows: -

$$D_I = \frac{\sum_{i=0}^{255} H_D(i)}{M \times N}$$

Where, M and N give the measurements of the image.

Quality of encryption increases with less DI. Irregularity for both algorithms between the encrypted and plain image increases.

Histogram Analysis

The Histogram in this case, uses a bar graph to fix occurrence of one grey level present. X - Axis shows all grey level values and Y - Axis represents a grey level occurrence.[2] Figure-5 & Figure-7 shows the original histograms of the brain and logo image, respectively whereas Figure-6 &Figure-8 shows the histograms of the encrypted form of both the images, respectively.

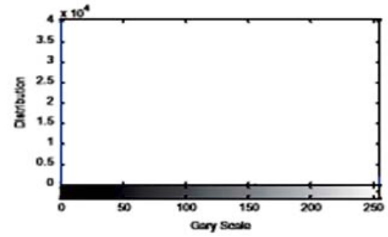


Fig. 5. Histogram of the brain image [2]

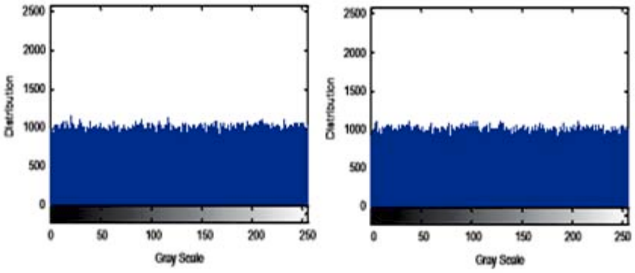


Fig. 6. Histogram of the encrypted brain image with RC6 and Rijndael algorithm in ECB mode using pre- processing [2]

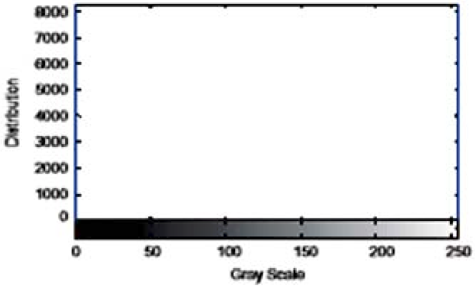


Fig. 7. Histogram of the logo image [2]

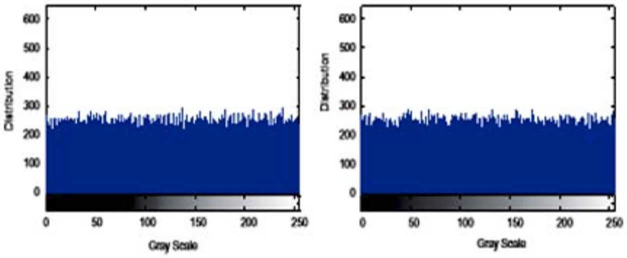


Fig. 8. Histogram of the encrypted logo image with RC6 and Rijndael algorithm in ECB mode using pre- processing [2]

Encryption Quality Metric

The Quality Metric DP is as follows: -

$$D_P = \frac{\sum_{C_I=0}^{255} |H(C_I) - H(C)|}{M \times N}$$

where,H(CI) is the histogram of the encrypted image[2]. The lower the value of encryption quality metric, better the encryption quality. Pre- processing enhances performances of encryption algorithms. Authors could have used Steganography to further impact their research of encrypting data in images of black and white backgrounds. The color block cipher algorithms of Rijndael and RC6 would have generated exceptional results using the features of Steganography.

2.2 Data Hiding in PDF Files

Portable Document Format (PDF) is a file format developed by Adobe Systems which is unique in nature and independent of any software, hardware or operating system. PDF secures data of all types such as text, images, graphics etc which makes the data in it very difficult to breach. In [5], the authors have developed two techniques to enhance the characteristics of data hiding in PDF files which was not satisfactory until then. The first technique looks for trash spaces in the file and replaces those spaces with encrypted version of data. The second technique manages to keep large amount of encrypted data without changing the usefulness of the file.Stego PDF Creator (SPDFC) as well as Secret Data Viewer (SDV)uses these techniques on Windows.

2.2.1 Finding Trash Spaces

The below equations are used to calculate the trash spaces in a PDF file: -

$$|A_i| = \sum_{j=1}^{n} |a_j|$$

where, |aj| is the extreme limit of jth element in Ai.[5]

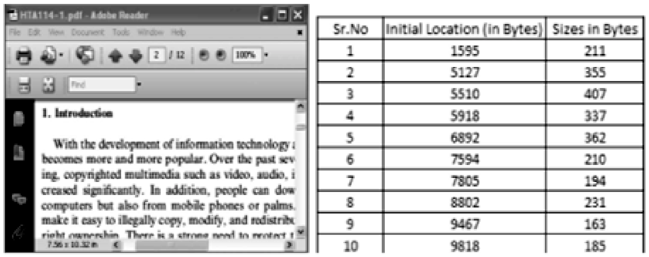
$$|X| = \sum_{i=1}^{n} |A_i|$$

The Cardinality of set X calculates complete length of PDF main body as well as the trash spaces.

The required steps of finding trash spaces are: -

```
I. Assume an array B[], Ascii_key
II. Enter statement"PDF File1"
III. Take for loop a=0 to 255
IV. Assume Ascii_key=a
V. Take for loop b=1 to length("PDF File1")
VI. If statement Ascii_key=ASCII("Character of PDF File1")
VII. Count the characters, cnt=cnt+1
VIII. Keep all locations in array B[]
IX. Stop if statement
X. Stop second for statement
XI. Stop first for statement
XII. Exit
```

From above technique, illustrated values of trash spaces in response to PDF Version 6 are shown in Figure - 9.


HTA114-1.pdf - Adobe Reader
File Edit View Document Tools Window Help
2 / 12
100%
Find
7.56 x 10.32 in

1. Introduction

With the development of information technology a becomes more and more popular. Over the past sev ing, copyrighted multimedia such as video, audio, i creased significantly. In addition, people can dow computers but also from mobile phones or palms. make it easy to illegally copy, modify, and redistribu right ownership. There is a strong need to protect t

Sr.No	Initial Location (in Bytes)	Sizes in Bytes
1	1595	211
2	5127	355
3	5510	407
4	5918	337
5	6892	362
6	7594	210
7	7805	194
8	8802	231
9	9467	163
10	9818	185

Fig. 9
(a) File size 373 KB (b) Trash spaces[5]

Steps for embedding of data in trash spaces: -

```
I. Enter statement"PDF file1"
II. Enter statement"Encrypted secret data1"
III. Enter statement"S_ key"
IV. Fetch Trash Space through code
V. Take for loop a=1 to length("Secret data1")
VI. Take for loop b=1 to length(B[])
VII. Change to "S_ key"
VIII. Change to "Secret data1"
IX. Stop second for loop
X. Stop first for loop
XI. Keep the statement"S file"
XII. Exit
```

Extraction Algorithm of Trash spaces

The steps proposed for extraction are: -

```
I. Assume an array T[], Ascii_key
II. Enter statement"PDF file1"
III. Enter S_key
IV. Take for loop a=1 to length("PDF file1")
V. If statement S_key=String("Characters of file")
VI. Keep the String("Characters of file") in array T[]
VII. Stop if statement
VIII. Stop for statement
IX. Exit
```

2.2.2 Data Appending

The second technique removes some anomalies of the first in the case, when the total size of the trash doesn't equal the data size. So, the steps required for appending secret data using the second technique are: -

```
I. Enter statement"PDF file1"
II. Enter statement"S_key"
III. Enter statement"Encrypted secret data1"
IV. Go toEOF("PDF file1")
V. Store statement"S_key
VI. Take for loop a=0 to length("Secret data1")
VII. Keep the "Originals"
VIII. Keepthe "Encrypting originals"
IX. Stop for statement
X. Keep the statement"S file"
XI. Exit
```

Extraction Algorithm of Data Appending

Steps proposed for finding secret data using the second technique: -

```
1. Enter statement"PDF file1"
2. Enter statement"S_key"
3. Take for loop a=0 to length("PDF file1")
4. If statement S_key=String("Characters of file")
5. Keep the String("Characters of file") in T[]
8. Stop if statement
9. Stop for statement
10. Reshuffle T[]
11. Exit
```

By combining both techniques technique, more data can be stored and hid.[5]

2.2.3Comparing Performance of Both Techniques with other known Techniques

On the Basis of Capacity to handle data:

Previous Techniques proposed by different authors - Most of the researchers took a picture as something which can store less data[5].

Trash Spaces and Data Appending Techniques

These techniques can handle large amount of data by taking more number of objects as in the case of first technique. In the second technique, more voluminous secret data can be embedded.

On the Basis of Compression to compress and decompress data in files

Previous Techniques proposed by different authors

Here, robustness of files was present but secret data was unchangeable.

Trash Spaces and Data Appending Techniques

Both these techniques support compression and decompression tests[5].

On the Basis of Visual Analysis to visually see data:

Previous Techniques proposed by different authors

There were changes which could visuallyseein those stegfiles of these techniques.

Trash Spaces and Data Appending Techniques

No visual changes seen in any of the two techniques.Though, the proposed techniques of the authors have many advantages as compared to previous traditional techniques but the different extraction algorithms used each for finding trash spaces and data appending have made it a slightly lengthy process. This could have been avoided if the authors would have used just one algorithm each for both the techniques.The extraction process could have been nested inside the main algorithm and would have sped up the process.

2.3 Securing Images through Recursive Visual Cryptography

Security is probably the most challenging and needed property in today's technological era. Many organizations have spent tremendous amount of money just to acquire this property for all their related projects. Without security, the data of any organization or a single unit is under threat of getting misplaced or completely taken out from existence. Such is the case with image authentication. Its security analysis is performed through a special method known as Visual Cryptography Scheme (VCS).

VCS known for its security uses the method of encryption to separate one image into many consecutive images. Advantage of VCS is that it provides the user with decryption of code which does not require any complex computation. In [6], the authors have explained the most widely used Gnanagurupuram- Kak (2, 2)-RVCSwhich is used to authenticate all kinds of images.

The Gnanagurupuram–Kak(2, 2)-RVCS methodmakes the images hidden in 2 places which enhances the images in an effective manner. Some notations required to define the encoding procedure are as follows: -

Jj- it is the jth secret image where j is in the range [1, N].
Q (-)- it is the operation of (2,2)-VCS which encrypts I into 2 different pales P1 and P2. For an assumed P1, Q (J, P1) =P2.
Pj, 1(Pj, 2) - 2 places of the jthstep in (2, 2)-RVCS which gives Jj=Pj, 2+Pj,2.
R1 (R2)- last of 2 places of (2, 2)-RVCS.
Encoding procedure is as follows: -

```
Enter: Jj where j is in the range [1,N].
Result: For R1 and R2,
1. Take an assumed P1, 1.
2. a) Take for loop a=1 to (N-1)
Do loop {
        Calculate Q(Jj,pj,1)=pj,2;
        Pj+1, 1=Pj, 1 concatenate Pj,2 };
  b) Calculate Q(PN,PN,1)=PN,2.
3. Result R1=PN, 1 and R2=PN,2.
```

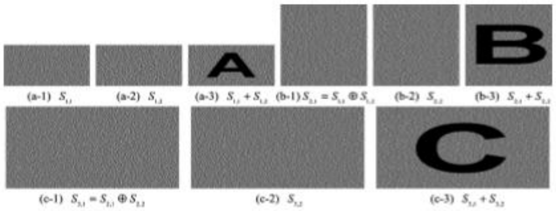


Fig. 10 [6]

Figure - 10 shows recursive hiding in images i) 2 places P1,1, P1,2 with result P1,1+ P1,2 ii) 2 places P2,1, P2,2 with result P2,1+ P2,2 iii) 2 places P3,1, P3,2 with result P3,1+ P3,2

Hence, RVCS has the capability to enhance information in images through recursive hiding.[6] But there are some limitations occurring due to some information present in sub-pixels. Hence, using this method for authentication purpose, the security should be taken under consideration.

Recursive Visual Cryptography is a vast subject inside Visual Cryptography. Though, the authors have mentioned that they will use the Gnanagurupuram algorithm but still the other techniques need to be mentioned in order to perform a comparative analysis and choose the best security authentication technique. This would have removed the few visible holes in the paper.

2.4 Cyber Crime through Encryption Techniques

Cybercrime is rapidly gaining momentum in the technology world. It's attracting many such individuals who either have been involved in thefts of any kind in their past or the ones who have a nag for engaging in criminal activities. Criminals use many different means to hide evidence on computers from law enforcement mainly through encryption and other such methods like steganography, digital compression, passwords etc. These techniques are making the law enforcement's tasks more difficult day-by-day so, there is a need to understand how these criminals work and to subsequently find a solution for the same. In [9], the authors have explained the above techniques in detail and how these affect the law enforcement efforts to counter.

2.4.1 Encryption

Real-Time Data Communications

The major effect of using encryption on real-time data communications is on wiretaps. Wiretap provides valuable information about the criminal's intentions, plans and any such rogue activities. Hackers use encryption on real-time data communications to prevent their communication channels to be intercepted by the law enforcement authorities.[9] Internet Relay Chat(IRC) is that channel which enable the hackers to compromise other government machines.

Electronic Mail

The criminals use many different ways to encrypt their data in emails. The most used technique is Pretty Good Privacy(PGP) which provides a key to perform data encryption.[9] This encryption technique is readily available in the Internet for free so, downloading is very easy. Electronic mail is very hard to trace.

Stored Data

This is the most commonly used technique by criminals to encrypt their stolen/ confidential data from the law enforcement.

Posts Online

Hackers/criminals create open forums such as Internet web sites to carry message across from one person to another.[9] This type of communication can be accessed by only those individuals who possess the decrypting key to that encrypted message.

2.4.2 Other Cryptographic Technologies

Passwords

Hackers/ criminals keeps their PC's password protected to keep out intruders. This is an easy and most effective way of securing one's identity from the rest of the world. Passwords are used much more often by hackers rather than encryption related techniques.

Compressing Digital Files

Digital compression compresses digital file's size preventing the loss of important details of the file. Criminals use compression for two benefits: -

a) A decompressed file makes it hard for the law enforcement authorities to seize crucial files.

b) Prior to encryption, it can make cracking of system difficult to conduct.

Steganography

Steganography is the method of hiding secret data into another data so that it is even more secured. Criminals use it to trick the concerned authorities into seeing non- existence of files in a hard-disk of computer. A cracker who does not possess the knowledge of the files can be easily mislead and forced to act in a way which can further make their target even more difficult to achieve.

The authors have stressed a lot on the ways criminals/ hackers use encryption techniques to steal & extract confidential Government and other important organization's data but not so much on the ways to counter such actions. There is a need to talk about both sides of the argument in such cases. The encryption techniques used by criminals can be countered in a similar manner by the law enforcement authorities using decryption (also part of encryption). Some of those techniques are talked about in the above research papers.

2.5 Hiding Secret Information in Digital Images

In [1], [3], [4], [7], we are able to see many different ways in which images are secured from interference of hackers and other such outside intruders. The concept of digital watermarking is used to allow the authorization of owner and prevent outside intrusion, random grids used to hide secret images and use of joint encryption techniques to provide the same property.

2.6 Mathematical Models to Enhance Visual Cryptography

In [8], [10], [13], [16], various mathematical models are proposed which enhance the cryptographic techniques by making them more reliable during experimentation. The VC schemes based on the equations derived in the models allow the transparencies of the techniques to freely occur and help perform their desired functions. The application of this is seen in [13].

2.7 Preventing Unauthorized Access at Sensitive Application Areas

In [11], [12], [14], [19], the authors talk about ways in which outside intrusion can be prevented in application areas like bank transactions, fingerprint scanning etc. The cryptographic techniques provide security but not necessarily define how hackers intrude into the system. The term phishing is used which occurs when a second user poses as a trustworthy entity to gather important information about the main user such as passwords, personal information etc.

2.8 Visual Cryptography Properties Used in Day-to-Day Application Areas

In [15], [17], [18], [20], the authors have used a new dimension to describe properties of visual cryptography in fields of multimedia and baseball. Cryptography can encrypt audio files more easily than text as audio files are more error tolerant. In baseball, the third- base coach gives visual signals to batters, pitchers etc during the course of the game. The halftone visual cryptography is used to encrypt secret data which is used in multimedia cryptography.

III. CONCLUSION

Applications of Visual Cryptography talked about in this review paper focus mainly on the use of encryption which is the most important feature of visual cryptography. The research papers reviewed above describe one of the best applications and aspects of visual cryptography. Future work can be done on [2],[5] to further enhance the use of application areas talked about in them.

REFERENCES

[1] ShyamalenduKandar, Arnab Maiti and Bibhas Chandra Dhara, “Visual Cryptography Scheme for Color Image Using Random Number with Enveloping by Digital Watermarking”, IJCSI International Journal of Computer Science Issues, vol.8, issue 3, no.1, May 2011.

[2] Som S., Banerjee Mandira, (2013) “Cryptographic Technique Using Substitution Through Circular Path Followed By Genetic Function”, International Journal of Computer Applications (IJCA), ISSN: 0975 – 8887, Impact Factor: 2.0973, ISBN: 973-93-80873-34-0 CCSN2012/Number 4, March 2013.

[3] Ibrahim F. Elashry, Osama S. Faragallah, Alaa M. Abbas, S. El-Rabaie&Fathi E. Abd El-Samie, “A New Method for Encrypting Images with Few Details Using Rijndael and RC6 Block Ciphers in the Electronic Code Book Mode”, Information Security Journal: A Global Perspective, 21:4, 193-205, 5 June 2012.

[4] Sachin Kumar and R. K. Sharma, “Recursive Information Hiding of Secrets by Random Grids”, Cryptologia, 37:2, 154-161, 1 April 2013.

[5] Hsien-Chu Wu, Hao-Cheng Wang and Rui-Wen Yu, (2008), "Color Visual Cryptography Scheme Using Meaningful Shares," in *Intelligent Systems Design and Applications, 2008. ISDA '08. Eighth International Conference*, vol.3, pp.173-178, 26-28 Nov. 2008.

[6] Rajesh Kumar Tiwari & G. Sahoo, “A Novel Methodology for Data Hiding in PDF Files”, Information Security Journal: A Global Perspective, 20:1, 45-57, 7 July 2013.

[7] Ching-Nung Yang &Tse-Shih Chen,“Security Analysis of Authentication of Images Using Recursive Visual Cryptography”, Cryptologia, 32:2, 131-136, 19 May 2014.

[8] Amit Phadikar& Santi P. Maity, “On Security of Compressed Gray Scale Image Using Joint Encryption and Data Hiding”, Information Security Journal: A Global Perspective, 20:6, 274-289, 11 Nov. 2011.

[9] Nuh Aydin, “Enhancing Undergraduate Mathematics Curriculum Via Coding Theory and Cryptography”, PRIMUS, 19:3, 296-309, 29 April 2013.

[10] Dorothy E. Denning & William E. Baugh Jr, “Hiding crimes in Cyberspace”, Information, Communication & Society, 2:3, 251-276, 2 Dec. 2015.

[11] Som S., Chatergee N. S., Mandal J. K., (2011) “Key Based Bit Level Genetic Cryptographic Technique (KBGCT)”, IEEE International Conference on Information Assurance and Security (IAS 2011), IEEE Explorer, ISBN: 978-1-4577-2154-0, p.p. 240 – 245, 5th to 8th December, 2011, Malacca, Malaysia.

[12] M. Sukumar Reddy and S. Murali Mohan, “Visual Cryptography Scheme for Secret Image Retrieval”, IJCSNS International Journal of Computer Science and Network Security, vol.14, no.6, June 2014.

[13] Subba Rao, V. Yengisetty and Bimal K. Roy, “Applications of Visual Cryptography”, International Journal of Parallel, Emergent and Distributed Systems, 26:5, pg. 429-442, 28 Oct. 2011.

[14] MeenakshiGnanaguruparan&SubhashKak, “Recursive Hiding of Secrets in Visual Cryptography”, Cryptologia, 26:1, 68-76, 4 June 2010.

[15] Dennis R. Mills, “Signals Intelligence and the Coder Special Branch of the Royal Navy in the 1950s”, Intelligence and National Security, 26:5, 639-655, 1 Dec. 2006.

[16] Gaurav Palande, ShekharJadhav, AshutoshMalwade, Vishal Divekarand Prof. S. Baj, “An Enhanced Anti-Phishing FrameworkBased on VisualCryptography”, International Journal of Emerging Research in Management &Technology, vol.3, issue 3, March 2014.

[17] Tim McDevitt & Tom Leap, “Multimedia Cryptology”, Cryptologia, 33:2, 142-150, 9 July 2009.

[18] Sian-Jheng Lin and Wei-Ho Chung, "A Probabilistic Model of Visual Cryptography Scheme With Dynamic Group," in *InformationForensicsand Security, IEEE Transactions on*, vol.7, no.1, pp.197-207, Feb. 2012.

[19] S. Som, S. Sinha, R. Kataria (2016) “STUDY ON SQL INJECTION ATTACKS: MODE, DETECTION AND

PREVENTION", International Journal of Engineering Applied Sciences and Technology, Indexed in Google Scholar, ISI etc., Impact Factor: 1.494, Vol. 1, Issue 8, ISSN No. 2455-2143, Pages 23-29, June - July 2016.

[20] Zhi Zhou; Arce, G.R.; Di Crescenzo, G., "Halftone visual cryptography," in *Image Processing, IEEE Transactions on*, vol.15, no.8, pp.2441-2453, Aug.2006.

[21] Wayne Patterson, "The Cryptology of Baseball", Cryptology, 35:2, 156-163, 11 April 2011.

[22] Ramya, J.; Parvathavarthini, B., "An extensive review on visual cryptography schemes," in *Control, Instrumentation, Communication and ComputationalTechnologies (ICCICCT), 2014 International Conference on*, vol., no., pp.223-228, 10-11 July 2014.

[23] Gupta, Himanshu; Sharma, Vinod Kumar; "ROLE OF MULTIPLE ENCRYPTION IN SECURE ELECTRONIC TRANSACTION", International Journal of Network Security & Its Applications, Nov 2011, pp: 89-96.

[24] Gupta, Himanshu; Sharma, Vinod Kumar; "Multiphase Encryption: A New Concept in Modern Cryptography", International Journal of Computer Theory and Engineering, Aug 2013, pp: 638-641.

[25] Som S., Mitra D., Halder J., (2008) "Session Key Based Manipulated Iteration Encryption Technique (SKBMIET)", IEEE International Conference on Advanced Computer Theory and Engineering (ICACTE 2008), ISBN No.: 978-0-7695-3489-3, pp: 694-698, 20-22, December 2008, Phuket, Thailand.

[26] Desiha, M.; Kaliappan, V.K., "Enhanced efficient halftoning technique used in embedded extended visual cryptography strategyfor effective processing", vol.5, 8-10 Jan. 2015.