Appositeness and usage of Visual Cryptography: An Exploration

M. Raghupathi, G. Geetha Sai Sruthi

Abstract*— *Visual cryptography is a cryptographic strategy which enables visual data to be scrambled so that unscrambling turns into a mechanical activity that does not require a PC. In this paper, we expect to think about the extraordinary application zones of Visual Cryptography. Visual Cryptography is a wide zone of research utilized in information stowing away, anchoring pictures, shading imaging, media and other such fields. Visual Cryptography comes in the field of information stowing away utilized in cybercrime, record positions and so on. This paper centers around the application zones of visual cryptography from four distinctive research papers/diaries which talk about the most critical application regions of visual cryptography.

I INTRODUCTION

Visual Cryptography is a cryptographic method which enables visual data to be encoded so that decoding turns into a mechanical activity that does not require a PC. In the present PC age, information security, covering up and every single such movement have progressed toward becoming most likely the most vital perspective for generally associations. These associations burn through a great many their cash to simply anchor their information. This direness has ascended because of increment in digital robbery/ wrongdoing. The innovation has developed so much that culprits have discovered numerous approaches to perform cybercrime to which the concerned experts have either less or not adequate answer to counter. Consequently, the technique for Cryptography gives the above answers. A standout amongst the most majorparts of cryptography is Visual cryptography. It has numerous use and application territories, for the most part utilizing its inward system called encryption. Some of those application zones are discussed in this exploration paper.Visual cryptography is utilized explicitly in the regions of Biometric security, Watermarking, Remote electronic casting a ballot, Bank client ID and so forth. This exploration paper contains 4 areas. Segment 2 discusses the related work and applications in the field of Visual Cryptography. Area 3 gives the Finish of the paper pursued by References.

Revised Manuscript Received on 14 August, 2019.

M.Raghupathi, Assistant Professor, Department Of Computer Science And Engineering, MallaReddy Engineering College For Women, Email id:mraghu30@gmail.com

G.GeethaSaiSruthi, Assistant Professor, Department Of Computer Science And Engineering, MallaReddy Engineering College For Women Email id: saigeeta44@gmail.com

II. RELATED WORK

2.1 Rijndael and RC6 Block Cipher

Data in various structures, for example, content, picture, sight and sound and so forth is a vital apparatus in the present everyday life. Thus,arise the need to ensure this data/information from outside impedance which can make a risk at a huge scale in numerous cases. In [2], the creators proposed two extremely proficient systems to encode pictures with few pictures utilizing Rijndael what's more, RC6 Square Figures in Electronic Code Square (ECB) Mode utilizing pre-handling. Pre-handling empowers the calculations to avert examples to rise in the pictures previously encryption.

Rijndael: The Rijndael square figure is an iterated square figure utilizing variable square and key size[2]. It is the main encryption mode utilizing parallel preparing. The square figure calculation gives mapping of plain content square to figure content square and subsequently, from figure content square to plain content square utilizing figure key. Rijndael bolsters all mixes of square and key sizes of numerous of 32 bits with least of 128 bits and most extreme of 256 bits.

RC6: The RC6 square figure depends for the most part on four working registers, each of 32 bits. It is a key having variable parameters for example, key and square size, number of rounds. RC6 encoded calculation is assigned as: - RC6 (w,r,b) where w is the word estimate, r is the quantity of rounds, b is the quantity 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.

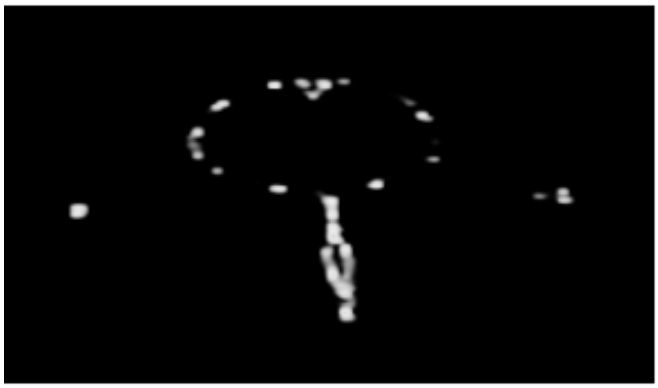


Fig. 1. Medical image of a brain with black area [2]Fig. 2. CS logo with white area [2]

Figure - 2 is an image consisting of two letters C & S with white area to be used for encryption.
Through the tests, it was inescapable that Rijndael and RC6 square figure calculations work effectively in ECB Mode utilizing pre-handling. Figure-3 &Figure-4 demonstrate the aftereffects of the above for the two pictures.

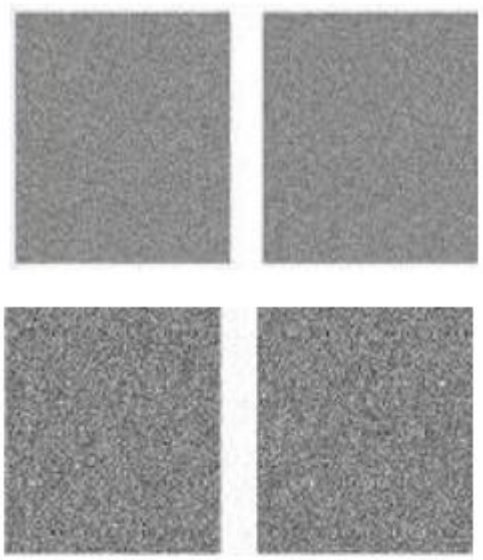


Fig. 3. Encrypted medical images with Rijndael and Fig. 4. Encrypted CS logo with Rijndael and RC6 algorithms in RC6algorithms in ECB mode using pre- processing [2] ECB mode using pre- processing [2]

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 for this situation, utilizes a reference diagram to settle event of one dim dimension present. X - Hub demonstrates all dark dimension esteems furthermore, Y - Hub speaks to a dark dimension occurrence.[2] Figure-5 and Figure-7 demonstrates the first histograms of the cerebrum and logo picture, separately though Figure-6 &Figure-8 demonstrates the histograms of the encoded type of both the pictures, separately.

where,H(CI) is the histogram of the scrambled image[2]. The bring down the estimation of encryption quality measurement, better the encryption quality. Pre-preparing upgrades exhibitions of encryption calculations. Creators could have utilized Steganography to additionally affect their examination of encoding information in pictures of highly contrasting foundations. The shading square figure calculations of Rijndael and RC6 would have produced remarkable outcomes utilizing the highlights of Steganography.

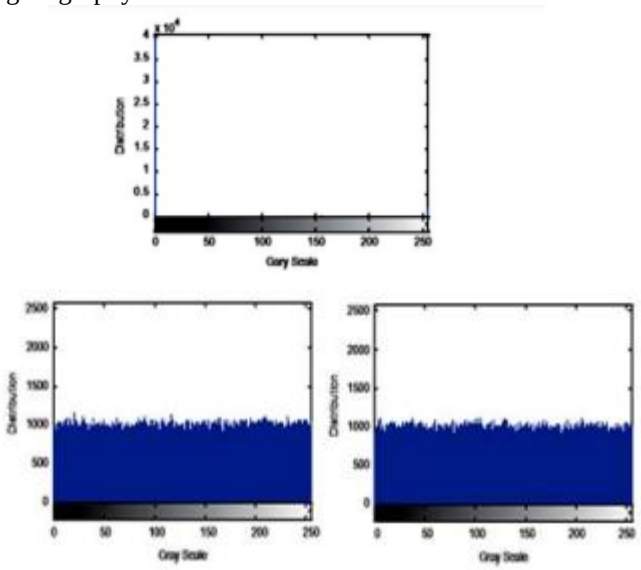


Fig. 5. Histogram of the brain image [2]Fig. 6. Histogram of the encrypted brain image with RC6 and Rijndael algorithm in ECB mode using pre- processing [2]

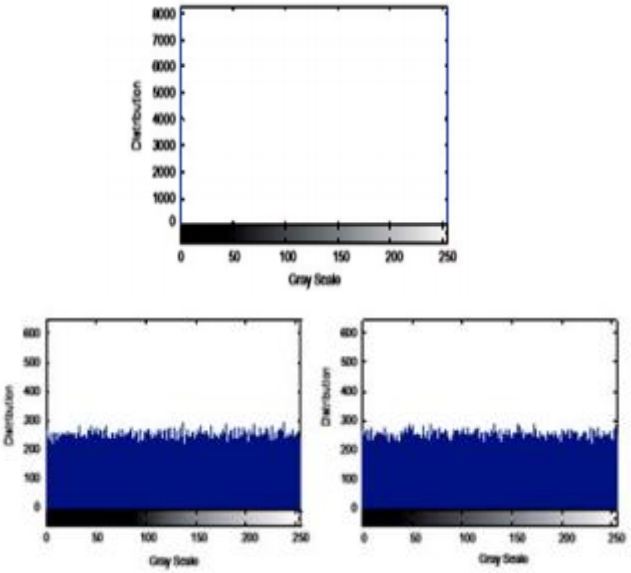


Fig. 7. Histogram of the logo image [2]Fig. 8. Histogram of the encrypted logo image with RC6 and Rijndael algorithm in ECB mode using pre- processing [2]

Encryption Quality Metric

The Quality Metric DP is as follows: -

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

2.2 Data Hiding in PDF Files

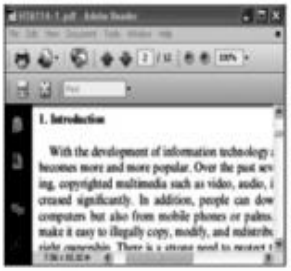
Portable Document Formate (PDF) is a document organize created by Adobe Frameworks which is one of a kind in nature and free of any product, equipment or working framework. PDF anchors information of different types, for example, content, pictures, designs and so on which makes the information in it extremely hard to rupture. In [5], the creators have created two procedures to upgrade the attributes of information covering up in PDF records which was not acceptable up to that point. The first procedure searches for waste spaces in the document and replaces those spaces with encoded rendition of information. The second strategy figures out how to keep expansive measure of encoded information without changing the helpfulness of the file.Stego PDF Maker (SPDFC) and additionally Mystery Information Watcher (SDV)uses these systems 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 statementAscii_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.



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: -
1.Enter statement"PDF file1"
2.Enter statement"Encrypted secret data1"
3. Enter statement"S_ key"
4. Fetch Trash Space through code
5. Take for loop a=1 to length("Secret data1")
6. Take for loop b=1 to length(B[])
7. Change to "S_ key"
8. Change to "Secret data1"
9. Stop second for loop
10. Stop first for loop
11. Keep the statement"S file"
12. Exit

Extraction Algorithm of Trash spaces

The steps proposed for extraction are: -
1.Assume an array T[], Ascii_key
2. Enter statement"PDF file1"
3. Enter S_key
4. Take for loop a=1 to length("PDF file1")
5. If statement S_key=String("Characters of file")
6. Keep the String("Characters of file") in array T[]
7. Stop if statement
8. Stop for statement
9. Exit

2.2.2 Data Appending

The second strategy evacuates a few inconsistencies of the first in the case, when the aggregate size of the junk doesn't equivalent the information estimate. Along these lines, the means required for adding mystery information utilizing the second strategy are:
1.Enter statement"PDF file1"
2.Enter statement"S_key"
3. Enter statement"Encrypted secret data1"
4.Go toEOF("PDF file1")
5. Store statement"S_key
6.Take for loop a=0 to length("Secret data1")
7. Keep the "Originals"
8. Keepthe "Encrypting originals"
9.Stop for statement
10. Keep the statement"S file"
11. 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 Execution of The two Strategies with other known Strategies Based on Ability to deal with information: Past Strategies proposed by various creators - Most of the specialists accepting an image as something which can store less data[5].

Trash Spaces and Data Appending Techniques
These strategies can deal with extensive measure of information by taking more number of items as on account of first method. In the second system, more voluminous mystery information can be inserted.
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.when contrasted with past conventional methods yet the unique extraction calculations utilized each to discover waste spaces and information adding have made it a marginally protracted process. This could have been kept away from if the creators would have utilized just one calculation each for both the techniques.The extraction process could have been settled inside the primary calculation and would have accelerated the procedure.

2.3 Securing Images through Recursive Visual Cryptography

Security is likely the most difficult and required property in the present mechanical period. Numerous associations have spent huge measure of cash just to get this property for all their related undertakings. Without security, the information of any association or a solitary unit is under risk of getting lost or totally taken out from presence. Such is the case with picture validation. Its security investigation is performed through an extraordinary technique known as Visual Cryptography Scheme (VCS).
VCS known for its security utilizes the strategy for encryption to separate one picture into numerous back to back pictures. Favorable position of VCS is that it gives the client decoding of code which does not require any perplexing calculation. In [6], the creators have clarified the most broadly utilized Gnanagurupuram-Kak(2,2)-RVCSwhich is utilized to validate a wide range of pictures.
The Gnanagurupuram– Kak(2, 2)- RVCS methodmakes the pictures covered up in 2 places which upgrades the pictures in an powerful way. A few documentations required to characterize the encoding methodology are as per the following: -
Jj – it is the 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 j^{th} step 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 fallowos: -
Enter: Jjwhere 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,1concatenate Pj,2};

b) Calculate Q(PN,PN,1)=PN,2.
3. Result R1=PN, 1 and R2=PN,2.

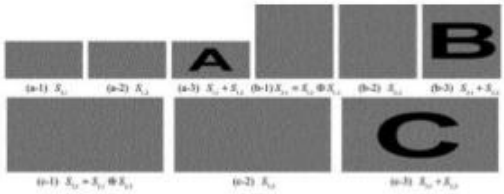


Fig. 10 [6]

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
Consequently, RVCS has the ability to improve data in pictures through recursive hiding.[6] But there are a few impediments happening because of some data present in subpixels. Henceforth, utilizing this strategy for validation reason, the security ought to be thought about.
Recursive Visual Cryptography is a huge subject inside Visual Cryptography. However, the creators have referenced that they will utilize the Gnanagurupuram calculation yet the other methods should be referenced so as to play out a relative examination and pick the best security verification strategy. This would have evacuated the few obvious gaps in the paper.

2.4 Encryption Techniques using in Cyber Crime

Cybercrime is quickly picking up energy in the innovation world. It's pulling in numerous such people who either have been engaged with robberies of any sort in their past or the ones who have a bother for taking part in criminal exercises. Hoodlums utilize a wide range of intends to conceal proof on PCs from law authorization mostly through encryption and other such techniques like steganography, computerized pressure, passwords and so forth. These systems are making the law authorization's undertakings more troublesome step by step in this way, there is a need to see how these culprits work and to in this way discover an answer for the equivalent. In [9], the creators have clarified the abovementioned strategies in detail and how these influence the law requirement endeavors to counter.

2.4.1 Encryption Real-Time Data Communications

The significant impact of utilizing encryption on continuous information correspondences is on wiretaps. Wiretap gives important data about the criminal's expectations, plans and any such rebel exercises. Programmers utilize encryption on constant information interchanges to keep their correspondence channels to be captured by the law authorization authorities.[9] Internet Transfer Chat(IRC) is that channel which empower the programmers to bargain other government machines.

Electronic Mail
The crooks utilize various approaches to scramble their information in messages. The most utilized strategy is Pretty Good Privacy(PGP) which gives a key to perform information encryption.[9] This encryption strategy is promptly accessible in the Internet for nothing along these lines, downloading is simple. Electronic mail is difficult to follow.

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

Posts Online
Programmers/criminals make open discussions, for example, Internet web destinations to convey message opposite one individual to another.[9] This sort of correspondence can be gotten to by just those people who have the unscrambling key to that encoded message.

2.4.2 Other Cryptographic Technologies

Passwords
Programmers/offenders keeps their PC's secret key secured to keep out gatecrashers. This is a simple and best method for anchoring one's personality from whatever is left of the world. Passwords are utilized considerably more frequently by programmers as opposed to encryption related strategies.

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 strategy for concealing mystery information into another information with the goal that it is considerably more anchored. Offenders utilize it to trap the concerned experts into seeing non-presence of documents in a hard-plate of PC. A wafer who does not have the learning of the documents can be effectively misdirect and compelled to act in a way which can additionally make their objective significantly more hard to accomplish.

The creators have focused on a great deal on the ways crooks/programmers utilize encryption strategies to take and concentrate classified Government and other critical association's information however not really much on the approaches to counter such activities. There is a need to talk about the two sides of the contention in such cases. The encryption methods utilized by culprits can be countered in a comparable way by the law implementation specialists utilizing unscrambling (likewise part of encryption). A portion of those strategies are discussed 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], different scientific models are proposed which upgrade the cryptographic strategies by making them more dependable amid experimentation. The VC plans dependent on the conditions inferred in the models permit the transparencies of the strategies to openly happen and help play out their coveted capacities. The use of this is seen in [13].

2.7 Preventing Unauthorized Access at Sensitive Application Areas

In [11], [12], [14], [19], the creators talk about manners by which outside interruption can be avoided in application territories like bank exchanges, unique mark filtering and so on. The cryptographic systems give security yet not really characterize how programmers barge in into the framework. The term phishing is utilized which happens when a second client acts like a dependable element to assemble critical data about the fundamental client, for example, passwords, individual data and so forth.

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

In [15], [17], [18], [20], the creators have utilized another measurement to depict properties of visual cryptography in fields of interactive media and baseball. Cryptography can scramble sound records more effortlessly than content as sound documents are more mistake tolerant. In baseball, the third-base mentor gives visual signs to hitters, pitchers and so on over the span of the diversion. The halftone visual cryptography is utilized to scramble mystery information which is utilized in sight and sound cryptography.

III. CONCLUSION

Utilizations of Visual Cryptography discussed in this audit paper center for the most part around the utilization of encryption which is the most vital component of visual cryptography. The examine papers checked on above depict truly outstanding applications and parts of visual cryptography. Future work should be possible on [2],[5] to additionally upgrade the utilization of use zones discussed 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. ElRabaie&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.