A GUI development of Visual Cryptography Scheme for User Authentication in MATLAB

Chanchal Kumari[1] Dr. Megha Mishra[2] Yamini Chouhan[3] Puajala Nanda Kishore[4] Dr. V. K. Mishra[5]
[1]M. Tech Research Scholar [2,5]Associate Professor [3,4]Assistant Professor
[1,2,3,5]Department of Computer Science & Engineering
[1,2,3,5]SSGI (FET), SSTC Bhilai, India [4]B.E.C Bapatla, A.P, India

Abstract— We present in this paper utilizing visual cryptography and undetectable computerized watermarking for user authentication in graphical user interface platform. Visual cryptography which enables visual data to be encoded so that unscrambling turns into the activity of the individual to decode by means of a sight perusing. In the proposed work, client mark will be installed inside the spread media. It might be content, pictures, sound, video and so on. Here we utilized spread picture for implanting information by utilizing a solitary piece LSB watermark addition calculation. After that the picture will be part into two offers share. Offers share will be later scrambled by utilizing a Column Shift Permutation calculation. Collector will decode the offers utilizing Column Shift Permutation calculation. Offers are gathered and stamp together by recipient to get spread picture. At that point mark will be de-installed from the spread picture. Information will be move utilizing correspondence media. Picture will be passed in progressively secure way with no bending. This strategy is exceptionally proficient and successful .The technique can be executed with least handling. Low PSNR is required in encryption so there fore obtained PSNR is 41.416 with respect to MSE is about 6.4123.

Keywords: Watermarking; Peak signal to noise ratio(PSNR); Visual Cryptography ; Graphical User Interfaces ; MSE (mean square errors); Authentication

I. INTRODUCTION

In these days security at different level such as data communication, cheaper internet connections, internet on things (IoTs) [1][2][3][5]and speedy software and hardware is play important role. Visual cryptography scheme is one of the solution to provide user authentication without mathematical operation is required in order to recover the secret data. Once sending information leakage temporally and noise is serious concerns occurs at the time of receiving the data (Bhagat et al. 2017)[6][7][8][9].

Over the accomplished few years, main problem in VC technique added during shares have contrast loss and pixel expansion, so therefore high computation space abd bandwidth involve during transmission (Jian et al.(2017) [2]. watermarking schemes proposed for the problems of attention the owner's absorb and the acknowledged customer's ownership.

VC has wide application such as :

1) In the processes of embedding splits .
2) In the business to send actual secret massage.
3) In the fields of data communication experts application.
4) In the Anti-Phishing systems.
5) Human machine identification.
6) Secure banking communication.
7) Defense system.

The VC arrangement abstraction has been continued to grayscale allotment images rather than double angel shares [10].Proposed VC schemes with accepted admission structures for grayscale allotment images. This adapted a gray-level angel into halftone images and again activated double VC schemes to accomplish grayscale shares. Although the abstruse angel is grayscale, shares are still complete by accidental double patterns accustomed beheld advice which may advance to suspicion of abstruse encryption [11].

II. RELATED WORK

In this study, a watermarking arrangement for assorted awning images and assorted owners is proposed. The proposed arrangement makes use of the visual cryptography (VC) technique, cipher text area, VC provides the adequacy to assure the absorb of assorted awning images for assorted owners, and the blow of the techniques are activated to enhance the robustness of the scheme [12][13][14][15]. Visual cryptography is a cryptographic technique which allows be considered encrypted in such a way that decryption becomes a automated operation that does not require a computer. The various algorithms that accept been fabricated to enhance the protection and that handle applications which need above ground similar of protection such as net cyber banking and amount banking[15][16][17][18]. Lakde et al. (2016) ,introduced a address for considered cryptography in which any display of angel can be called as a password, images again disconnected and again administer Shamir and M K Reddy encryption and decryption techniques[Reddy et al.(2014) ,The (t, n) beheld cryptography (VC) is a abstruse stacking of t-1 any out of transparencies reveals the administration arrangement area a abstruse angel is encoded into transparencies, and the abstruse image. The stacking of or beneath transparencies is clumsy to abstract any advice about the abstruse [19][20][21][22].

A. Problem Identification

1) It is not able to maintain the contrast quality of analyze image after decryption because of stego attacks.
2) It need to preserve the contrast quality of original images and provide a higher security.
3) Still this model security for the shared images got reduced.
4) The main problem of AES(Advance encryption standard) is error propagation stenography involve LSB(Less significant bits).
5) Variation of secret sharing scheme based on secret information such as SS scheme based on computer where number of infinity field.

In Section III, we accord some simulations for the proposed scheme. In Section IV, we draw some comparisons with account to the robustness and capability with some accepted

GUI based watermarking schemes. Finally, we accord a conclusion in Section V.

III. PROPOSED METHODOLOGY

In this scheme, authentication is provided by embedding and encryption of picture. The size of authentic photograph after embedding is remains unchanged in order that hacker cannot understand the image can be stegoimage. For that user signature can be embedded within the cowl media. The signature can be embedded into the quilt image via the usage of a single bit LSB watermark insertion algorithm. Stegoimage can be generated after which it is cut up into stocks. Percentage can be encrypted by using using a Column Shift Permutation encryption set of rules. Encrypted proportion could be ship to the receiver. Instead of using key for encryption as well as decryption, right here seed matrix is used at sender and receiver aspect for encryption and decryption to offer extra authentications. Figure 1 shows generation of share image in visual cryptography.

This stego picture is de-embedded with the aid of the use of the equal unmarried least massive bit watermark insertion algorithm. Subsequently, we get the separate cowl image and secret photo. The useful requirements may be technical info, records manipulation and different unique capability of the assignment is to provide the records to the person.

Non practical requirements in systems engineering and necessities engineering, a non-functional requirement is a requirement that specifies standards that can be used to decide the operation of a machine, in preference to precise behaviours:

A. Availability:

A gadget's "availability" or "uptime" is the amount of time this is operational and to be had to be used. It's associated with is the server presenting the service to the customers in showing photographs. As our machine may be utilized by thousands of customers at any time our device should be to be had continually. If there are any cases of updations they need to be executed in a quick c programming language of time without interrupting the normal services made available to the customers.

B. Performance:

Specifies how well the software utilizes scarce sources: CPU cycles, disk area, memory, bandwidth and so forth. All of the above mentioned sources can be successfully utilized by performing most of the validations at patron side and lowering the workload on server by means of using JSP as opposed to CGI that's being applied now.

C. Flexibility:

If the organization intends to growth or increase the functionality of the software after it's miles deployed, that ought to be planned from the start; it affects picks made during the design, improvement, checking out and deployment of the device. New modules may be without problems included to our machine without traumatic the existing modules or modifying the logical database schema of the present packages.

D. Portability:

Portability specifies the ease with which the software may be established on all vital structures, and the structures on which it's miles predicted to run. through the usage of suitable server variations released for exceptional systems our mission may be effortlessly operated on any operating system, consequently may be stated distinctly portable.

E. Scalability:

Software program this is scalable has the ability to handle a wide variety of gadget configuration sizes. The non-functional necessities ought to specify the approaches in which the gadget can be expected to scale up (through increasing hardware ability, adding machines and so on.). Our system may be without problems expandable. Any additional requirements such as hardware or software program which increase the overall performance of the system can be without difficulty introduced. A further server could be useful to hurry up the application.

F. Performance:

The performance constraints specify the timing characteristics of the software. Making the application shape filling process through on line and presenting the invigilation list records and exam corridor listing is given high precedence as compared to different offerings and may be diagnosed as the essential issue of the gadget.

G. Phases of System Design and implementation

1) Authentication:

The objective of authentication is done to identity of the data, image or whatever entities. Here authentication is mainly done at transmitter as well as the receiver for the security purpose.

2) Embedding:

An embedding here both secret image and cover image is taking such that secret image hiding behind the cover image using single bit least significant watermark insertion algorithm and stego image will be generated. Both files are saved with their respective extension.

3) Share Generation:

The stego image will be split into two parts. The share having same size and blur shares will be generated.

For all k there exists a general construction of k-out-of-k visual secret sharing scheme, the image sel expansion must use at least 2k-1 image sels , and the relative contrast should be 1/2k-1 . There is a need to construct two collections of k x 2k-1 Boolean matrices i.e. S0 and S1.

1) S0 is Handles the white image sels.
2) S1 is Handles the black image sels.

All 2k-1 columns have an even number of 1˝s in S0 and odd number of 1˝s in S1 and no two k rows are same in both S0 & S1. C0 and C1 contains all permutations of columns in S0 & S1. Properties of k-out-of-k Scheme

1) Image sel Expansion m=2k-1, (m should be as small as possible)
2) Relative Contrast α =1/2k-1, (α should be as large as possible)

3) r, the size of the collections. C0 and C1 (they need not be the same size, but in all of our constructions they are). Here r =2k-1!
4) logr is number of random bits needed to generate share.

We need two collections of 5 × 16 Boolean matrices and, contains all permutations of columns in and, by these two matrices we can design the shares of black and white image sels. Similarly as above, we can apply recursive scheme for any k-out-of-k scheme.

Figure 1 shows generation of share image in visual cryptography.

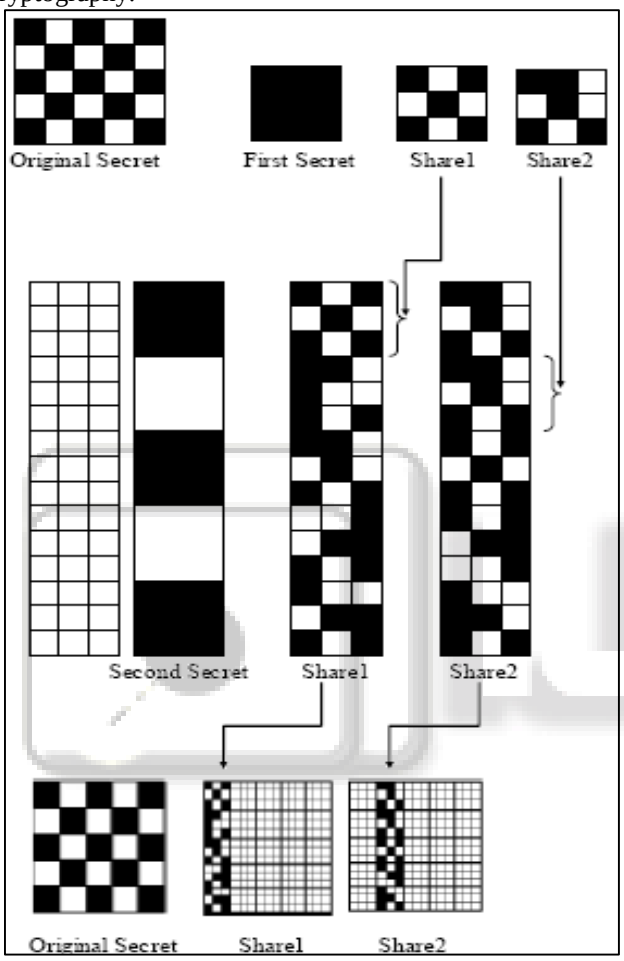

Fig. 1: Generation of share image in Visual Cryptography.

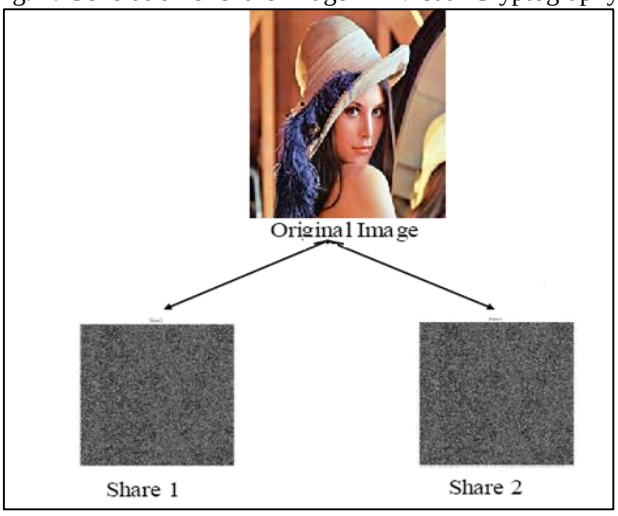

Fig. 2: Generation of stego picture.

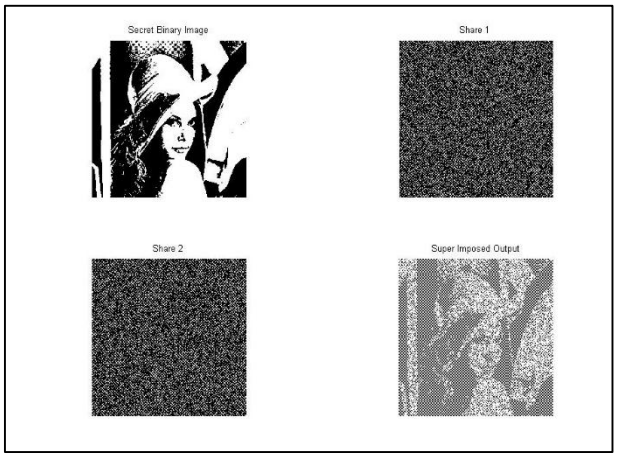

Fig. 3: Method for technology of Stego picture.

H. Algorithms

//Algorithm For Technology Of Stego Picture//
start.

1) Step 1-Take cover image and secret image.
2) Step 2-Loop for embedding
a) Get a imagesel from SI (secret picture)
b) Convert it into Binary that's of 8 bit
c) Extract 1-LSB from inexperienced aircraft of cowl photograph and 1-LSB from secret imaged. Perform addition of final bits of both images
3) Step 3- Stego picture can be generated.

prevent.

Figure 2 shown is a generation of stego picture which is share 1 and share 2.

//Algorithm For Proportion Generation //
begin.

1) Step 1- Take Stego photograph as enter.
2) Step 2- Convert it into eight-bit binary format.
3) Step 3- Separate the even-atypical little bit of photograph.
4) Step4- Fill the even-unusual clean position with padding 0 bit.
5) Step five- proportion 1 and share 2 generated
stop.

Figure 3 shows the method for technology of Stego picture.

//Set of Rules For Encryption Of Proportion//
begin.

1) Step 1-Take share 1(C1) and share 2(C2).
2) Step 2- constitute it into matrix shape.
3) Step three-Take seed matrix R.
4) Step 4- RC1=R - C1 or RC2= R - C2.
5) Step 5- observe column shift and transposition on RC1 and RC2.
6) Step 6- Encrypted stocks are fashioned forestall.

To get better the duvet image and secret photograph the opposite technique of set of rules can be observed.

IV. Result and Discussion

Excessive PSNR method proper image pleasant and much less blunders added to the photograph. In case of loss less compression PSNR may be high. if PSNR is high higher for Compression and Stegnography but encryption idea PSNR very low is better. Figure 4 is stego image is generated in GUI MATLAB. Lena image is input and out is text image. Peak

signal to noise ratiois calculated generally in logarithmic (dB) scale is a metric use to degree the fine of any photograph reconstructed, restored or corrupted image with respect to its reference or floor reality picture. it's miles a full reference photograph great measure defined because the most cost of maximum sign strength with admire to MSE (mean square errors) assumed as noise energy. For 8-bit picture most sign strength is (2^(8-1))^2 i.e. 255^2. further MSE may be calculated as the square difference among reference image and reconstructed/restored image in figure 5. hence a better cost of PSNR shows that the photo is of higher satisfactory and vice-versa. A 20 dB or better PSNR suggests that the image is of good excellent. PSNR excessive means: suggest square errors among the authentic image and reconstructed photo is very low. It means that the the has been nicely restored. inside the different manner, the restored picture best is higher. MSE is zero method no noise is present within the sign .There top noise to sign ratio have no importance.we will select both colour photo or gray scale photograph as input.

Figure 6. is retrieval secret image in GUI developments.

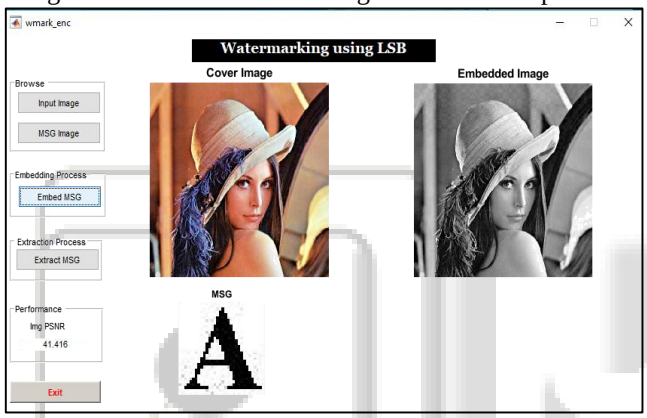

Fig. 4: Stego image is generated.

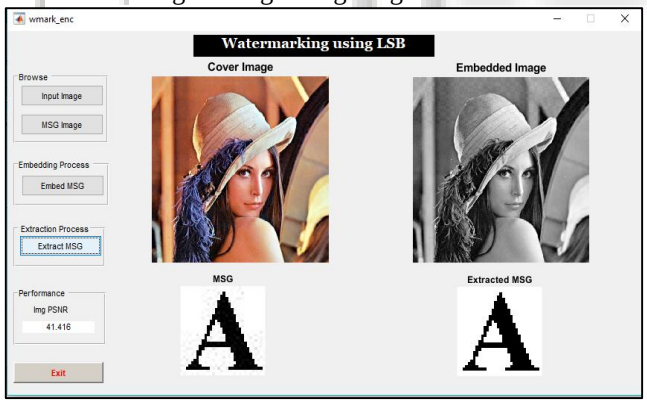

Fig. 5: Retrieval secret image.

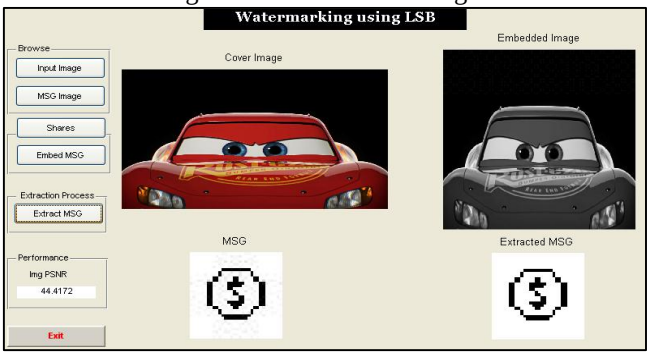

Fig. 6: Retrieval secret image.

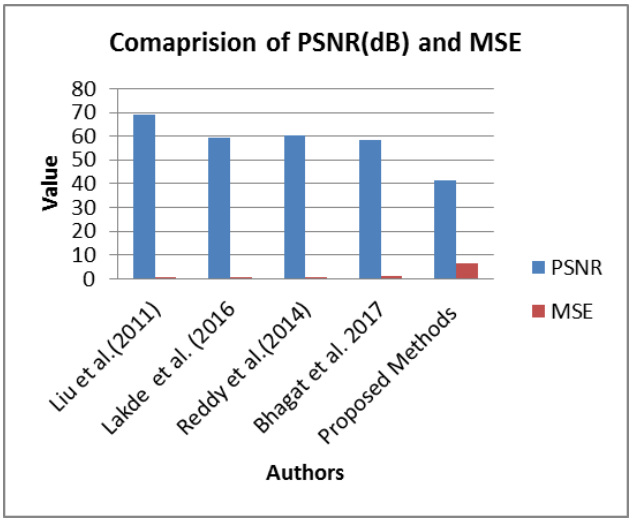

Fig. 7: Comparison of our methods with previous work.

Figure 7 and table I shows the Comparison of our methods with previous work.

Authors Name & Comparison Parameter	Liu et al.(2011)	Reddy et al.(2014)	Lakde et al. (2016)	Bhagat et al. 2017	Proposed Methods
PSNR	69.2633	60.345	59.263	58.2658	41.416
MSE	0.007186	0.065025	0.08186	0.096939	6.4123
Contrast improvement.	No	No	No	YES	YES
Share size improvement	No	No	No	YES	YES
Applications	Compression and Stegnography	Compression and Stegnography	Compression and Stegnography	User authentication	User Authentication

Table 1: Comparison of our methods with previous work

V. CONCLUSIONS

In this paper, it's miles apparent that loads of time and effort has reduced to visual secret sharing using GUI trends. Some of the schemes supplied work extremely nicely and the cutting-edge country of the art strategies have tested to be very useful for many packages, including verification and authentication. Evaluation development and share length improvement, wider variety of appropriate image kinds (binary to colour pics), efficiency of VC schemes, capability to percentage a couple of secrets and techniques is blessings of GUI implementation.

Basically the most vital part of our scheme is the contrast of the recovered secret from a selected set of shares.

Best schemes offer an excessive comparison whilst the secret has been recovered. but, a tradeoff is required in a few schemes relying on the size of the stocks along with the variety of secrets and techniques which may be concealed. Mainly within extended visual cryptography schemes, assessment is of principal significance. Ensuring the bottom pictures absolutely disappear and a clean secret is recovered which will be every other high first-class photo is vitally vital. The comparisons show that ourscheme has many good properties.

REFERENCES

[1] Ratheesh V.R., Jogesh J., Jayamohan M.," A Visual Cryptographic Scheme For Owner Authentication Using Embedded Shares", Indian Journal of Computer Science and Engineering (IJCSE) Vol.5, No.5, Oct-Nov, 2014.
[2] Nayan A. Ardak," Visual Cryptography Scheme for Privacy Protection", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014.
[3] Praveen Kumar. P," User Authentication using Visual Cryptography", 2015 International Conference on Control, Communication & Computing India (ICCC) ,19-21 Nov,2015.
[4] Chandrashekhara and Jagdisha," Secure Banking Application Using Visual Cryptography Against Fake Website Authenticity Theft", Vol. 2,Issue -2,2013.
[5] Sruthy K Joseph, Ramesh R," Random Grid Base Visual Cryptography Using A Common Share", Conference of computing and network communication (CoCoNet'15), Dec.16-19,2015.
[6] Patel Roshni, Prof. Aslam Durvesh, Prof. Aslam Durvesh,PatelUrvisha," Lossless Method for Data Hiding In Encrypted Image", IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems ICIIECS'15.
[7] F. Liu and C. -. Wu, "Robust visual cryptography-based watermarking scheme for multiple cover images and multiple owners," in IET Information Security, vol. 5, no. 2, pp. 121-128, June 2011.doi: 10.1049/iet-ifs.2009.0183.
[8] Long Bao, Yicong Zhou* and C. L. Philip Chen," A lossless (2,8)-chaos-based secret image sharing scheme", 2014 IEEE International Conference on Systems, Man, and Cybernetics October 5-8, 2014, San Diego, CA, USA.
[9] Y.C. Hou, P.M. Chen, An asymmetric watermarking scheme based on visual cryptography, in: IEEE International Conference on Signal Processing Proceedings, vol. 2, 2000, pp. 992–995.
[10] C.C. Wang, S.C. Tai, C.S. Yu, Repeating image watermarking technique by the visual cryptography, IEICE Trans. Fund. E83-A (8) (2000) 1589–1598.
[11] C.C. Chang, H.C. Wu, A copyright protection scheme of images based on visual cryptography, Imaging Sci. J. 14 (2001) 141–150.
[12] Lakde, N. K., & Shelke, P. B. Visual Cryptography Scheme with Authentication Using Shamir Andmk Reddy Techniques.
[13] Reddy, M. S., & Mohan, S. M. (2014). Visual Cryptography scheme for Secret image retrieval. International Journal of Computer Science and Network Security (IJCSNS), 14(6), 41.
[14] Naor, M. and Shamir, A. 1995. Visual Cryptography, in Advances in Cryptology – Eurocrypt. A. De Santis, Ed., Vol. 950 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, pp 1-12, 1995.
[15] 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.
[16] 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.
[17] Vaishali Bhagat, Rida Ansari, Roshani Thakre, Neha Patiye, Snehal Kolte and Latika Chaudhari, "A Visual Cryptography Scheme for User Authentication", International Journal on Recent and Innovation Trends in Computing and Communication, 5:2, pg. 168-172, 2017.
[18] Gaurav Palande, ShekharJadhav, Ashutosh Malwade, Vishal Divekarand Prof. S. Baj, "An Enhanced Anti-Phishing Framework Based on Visual Cryptography", International Journal of Emerging Research in Management &Technology, vol.3, issue 3, March 2014.
[19] Sian-Jheng Lin and Wei-Ho Chung, "A Probabilistic Model of Visual Cryptography Scheme With Dynamic Group," in Information Forensics and Security, IEEE Transactions on, vol.7,no.1, pp.197-207, Feb. 2012.
[20] D. S.Wang, F. Yi, and X. Li, "On general construction for extended visual cryptography schemes," Pattern Recognit., pp. 3071–3082, 2009.
[21] Z. Zhou, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography,"IEEE Trans. Image Process., vol. 18, no. 8, pp. 2441–2453, Aug. 2006.
[22] E. Myodo, S. Sakazawa, and Y. Takishima, "Visual cryptography based on void-and-cluster half toning technique," in Proc. IEEE Int. Conf. Image Process., 2006, pp. 97–100.

