ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

Enhanced the Performance of Visual Cryptography Using Watermarking Technique

Ranjan Kumar, Prof.Aishwarya Mishra

M.Tech Student, Dept. of Computer Science & Engineering, IES College of Technology, Bhopal, India

Associate Professor, Dept. of Computer Science & Engineering, IES College of Technology, Bhopal, India

ABSTRACT: Share generation play an important role in text cryptography and visual cryptography. The generation of share prevent form cheating of authenticated data from during the transmission of data. Share generation for the visual cryptography can also be done by the concept of watermarking using some watermarking technique. We can use these watermarked shares for retrieving the hidden information. This effort can generate the meaningful shares rather than some shares having no information. Fraudulent participants, however, may provide a fake shadow in order to fool others. Consequently, cheating prevention has become a critical essential for secret sharing systems. In this article, the authors propose an efficient image secret sharing scheme that can resist cheating attacks. The simulator shows that the novel scheme is sensitive to cheating detection and cheater identification. In particular, the new method allows an authorized participant to reveal a lossless secret image and to further restore the valued host image without distortion. The reversibility of the secret sharing system provides practicability and widespread potential for preserving medical images, military images and artistic images.

KEYWORDS: Visual Cryptography, Watermarking, Geometrical Attack Share Generation

I. INTRODUCTION

A visual secret sharing method, namely visual cryptography (VC), which can encode a secret image into n noise-like shares. The secret image can be decrypted by the human eye when any k or more shares are stacked together. The greatest advantage of this decryption process is that neither complex computations nor any knowledge about VC are needed. It is a simple and safe secret sharing method for the decoding of secret images when computer-resources are lacking. However, since VC uses a pixel expansion method to decompose the secret image, the share-images are larger than the original secret image. The drawbacks of this are wastage of storage space, image distortion and the share-images are difficult to carry. Since the concept of visual cryptography was first proposed, there have been several studies making efforts to deal with the pixel expansion problem [2, 11]. Most of these have fallen into the category of probability visual cryptography schemes. An encryption algorithm is proposed to hide the shared pixels in the single image random dot stereogram's (SIRDSs). Because the SIRDSs have the same 2D appearance as the conventional shares of a VCS, this paper tries to use SIRDSs as cover images of the shares of VCSs to reduce the transmission risk of the shares. Visual secret sharing (VSS), which is also called visual cryptography (VC), is a technique of cryptography which prevents a secret from being modified or destructed by using the notions of perfect cipher and human visual system. For a general scheme of (k, n) threshold, a secret image is encrypted into n random-looking images, also called shares or shadows. These n shares are then distributed to n associated participants. To visually reveal the secret, any k or more shares are required to stack together. But any k or less shadows give no clue about secret. Compared with some conventional encryptions such as DES and AES, VSS offers unbreakable encryption if a meaningless share contains truly random pixels such that it can be seen as a one-time pad system. Without using a computational device and crypto-graphic knowledge in decryption, VSS technique is effective and suitable for certain practical applications. In section two discuss the related work and in section III. In section IV discuss the proposed methodology. In section V discuss the experimental result and finally discuss conclusion and future work in section V.

Copyright to IJIRCCE

DOI: 10.15680/IJIRCCE.2017. 0506094

II. RELATED WORK

In this section discuss the related work in the field of visual cryptography for the image encryption and decryption. The visual cryptography used for the process of share generation. The distributed share generation used for the purpose of authentication and authorization. Some common work related in this filed discuss here.
Young-Chang Hou, Shih-Chieh Wei, and Chia-Yin Lin [1] Et al. A probability allocation method is then proposed which is capable of producing the best contrast in both of the share-images and the stack-image. With their method, not only can different cover images be used to hide the secret image, but the contrast can be set as needed. The most important result is the improvement of the visual quality of both the share-images and the stack-image to their theoretical maximum. Their meaningful visual secret sharing method is shown in experiments to be superior to past methods. visual secret sharing scheme, not only maintains the security and pixel non-expanding benefits of the random-grid method, but also allows for the production of meaningful share-images, while satisfying the requirements of being easy to carry and easy to manage. Moreover, all pixels in the cover-image and the secret image are used to perform encryption, which ensures that the contrast on the share-images and the stack-image can reach the theoretical maximum. Their method also removes some unnecessary encryption restrictions which makes the encryption process more flexible.
Kai-Hui Lee, Pei-Ling Chiu [2] Et al. A binocular VCS (BVCS), called the (2, n)-BVCS, and an encryption algorithm are proposed to hide the shared pixels in the single image random dot stereogram’s (SIRDSs). Because the SIRDSs have the same 2D appearance as the conventional shares of a VCS, this paper tries to use SIRDSs as cover images of the shares of VCSs to reduce the transmission risk of the shares. The encryption algorithm alters the random dots in the SIRDSs according to the construction rule of the (2, n)-BVCS to produce nonpixel expansion shares of the BVCS. Altering the dots in a SIRDS will degrade the visual quality of the reconstructed 3D objects. Hence, they propose an optimization model that is based on the visual quality requirement of SIRDSs to develop construction rules for a (2, n)-BVCS that maximize the contrast of the recovered image in the BVCS.

Xiaotian Wu, DuanhaoOu, Lu Dai, Wei Sun [3] Et al. A novel (2, 2) generalized RG-based VSS is introduced. By adopting the (2, 2) VSS, they describe, a XOR-based meaningful VSS where shares with meaningful contents are constructed. Moreover, superior visual quality is provided by this method as well. firstly introduces a (2, 2) generalized RG-based VSS, where the average light transmission of a share be-comes adjustable. By recursively applying the (2, 2) scheme for n − 1 times, a (n, n) generalized RG-based VSS is pro-posed. And the (n, n) scheme is proved to be a valid construction of XOR-based VSS but with meaningless shares.

Gayathri Soman, Mr. Jyothish K John [4] Et al. The natural shares which are not altered are diverse and innocuous, thus greatly reducing the transmission risk problem. Also proposes a better secure way to hide the noise like share to reduce the transmission risk problem for the share. Experimental results show that the proposed approach is an excellent solution for solving the transmission risk problem for the VSS schemes.
The method discussed uses a VSS scheme which can share digital image by diverse image media. This method can share one digital secret image using n-1 natural images and one noise share. The natural shares can be photos or hand-painted pictures in digital form or in printed form. The noise like share is generated using the secret image and the natural images. The media that include randomly chosen images are unaltered in the encryption phase. It uses only one noise like share regardless of the number of participants .This method is the first attempt to share images via heterogeneous carriers in a VSS scheme.Also proposes an efficient method to hide the noise like share.
Amitava Nag, Sushanta Biswas, Debasree Sarkar, ParthaPratimSarka [5] Et al. They deals with a general (k, n) secret image sharing scheme for gray scale images with both low reconstruction complexity and preservation of the fault tolerance property. Moreover, the proposed sharing generation technique can also be applied on color images. A typical (k, n) secret sharing scheme provides a high fault-tolerant property due to its distributed storage mechanism. They discussed here, a new (k, n) secret sharing scheme, based on a Boolean operation. In the proposed scheme even if n – k shares are lost or corrupted, the remaining k shares are sufficient to recover the secret. Moreover, the reconstruction complexity of the method proposed is O(n) due to its Boolean operation. These are the main advantages of their proposed scheme compared to the existing methods. Moreover, their secret sharing can also be applied on colour images and it produces excellent results.

Juby Justin and Giss George [6] Et al. The advantage of the visual secret sharing scheme is its decryption process i.e. to decrypt the secret using Human Visual System without any computation. Traditional Visual Cryptography suffers from share identification problem. This problem can be solved by extended visual cryptography (EVCS), which adds a meaningful cover image in each share. But most EVCS for general access structures suffer from pixel expansion problem. This paper proposes a general approach to solve above mentioned problems. This approach can be used for color secret images.

Anran Wang, Shuai Ma, Chunming Hu, JinpengHuai, Chunyi Peng, Guobin Shen [7] Et al. They aim to boost the throughput over screen-camera links by enhancing the transmission reliability. To this end, they discuss RD Code, a robust dynamic barcode which enables a novel packet-frame-block structure. Based on the layered structure, they design different error correction schemes at three levels: intra-blocks, inter-blocks and inter-frames, in order to verify and recover the lost blocks and frames. Finally, they implement RD Code and experimentally show that RD Code reaches a high level of transmission reliability and yields at least two-fold improvement of transmission rate, compared with the existing state-of-the-art approach COBRA.

Bharanivendhan N and Amitha T [8] Et al. The secret image can be recovered simply by stacking the shares without any complex computation involved. However previous approach suffers a security, pixel expansion and noise problem. The proposed system consists of two phases. At the sender side, the input secret image generates the four meaningless shares based on GAS algorithm is done in the first phase. In the second phase, the cover images are added in each shares directly by using stamping algorithm and distributed the embedded images to the participants. At the receiver side, the embedded images can be processed to extract the covering images from the generated shares and the secret images can be retrieved by overlapping the shares in the correct order. The password authentication is also provided at both the sender and receiver side. The proposed system provides high security, increase in the number of shares and reduce the pixel expansion problem and high resolution to visualize the secret image.

Jun Kong, Omer Barkol, Ruth Bergman, AyeletPnueli, Sagi Schein, Kang Zhang, and Chunying Zhao [9] Et al. They develop a robust and formal approach to recovering interface semantics using graph grammars. Because of the distinct capability of spatial specifications in the abstract syntax, the spatial graph grammar (SGG) is selected to perform the semantic grouping and interpretation of segmented screen objects. Instead of analyzing HTML source codes, they apply an efficient image-processing technology to recognize atomic interface objects from the screenshot of an interface and produce a spatial graph, which records significant spatial relations among recognized objects. A spatial graph is more concise than its corresponding document object model structure and, thus, facilitates interface analysis and interpretation. Based on the spatial graph, the SGG parser recovers the hierarchical relations among interface objects.

Wazir Zada Khan,Yang Xiang, Mohammed Y Aalsalem, Quratulain Arshad [10] Et al. They discuss a flip visual cryptography (FVC) scheme with perfect security, conditionally optimal contrast, and no expansion of size. The proposed FVC scheme encodes two secret images into two dual-purpose transparencies. Stacking the two transparencies can reveal one secret image. Flipping one of the two transparencies and then stacking with the other transparency can reveal the second secret image. The proposed scheme is proved to have conditionally optimal contrast: its contrast is optimal if the double-secrets non-expanded FVC scheme is required to have perfect security. The perfect security is also proved.

Opaque-oriented and non-opaque-oriented FVC schemes are both introduced. They have proved that both schemes satisfy perfect security and they are conditionally optimal in contrast. The generated transparencies do not lead to any expansion of size. The experimental results show the revealing of double-secrets via flipping and stacking the transparencies together. Just like other VC methods, the whole decoding process uses no computer or any computation; so the decoding is very fast, and can be used in environment where computer is not stable or available. Due to the double-secrets feature of the proposed method, one of the applications is the double checking of ownership for personality identification. Since the size is non-expanded, the space needed to carry a transparency to a meeting is economic.

Wazir Zada Khan,Yang Xiang, Mohammed Y Aalsalem, Quratulain Arshad [11] Et al. They have described comprehensively all those systems which are using smart phones and mobile phone sensors for humans good will and better human phone interaction. The state of the art in research and development of Mobile Phone Sensing Systems. Smart Phones are getting smarter because of all the sensors being added to them. It is shown that the current status of Smart Phone sensors has the potential to revolutionize various fields of human life. In-built mobile phone sensors have many such capabilities that can improve people's lives cutting down the time it takes to find things, to prevent people from getting lost, improve health conditions, and even more serious applications are emerging that could actually save lives.

J. Galbally [12] Et al. According to author, the goal of this paper is to provide a comprehensive overview on the work that has been carried out over the last decade in the emerging field of antispoofing, with special attention to the mature and largely deployed face modality.

.

Snehal N. Meshram and Sneha U. Bohra [13] Et al. They discussed, Simple Visual Cryptography is very insecure. Variable length key based Visual Cryptography for color image uses a variable length Symmetric key based Visual Cryptography scheme for color images where a secret key is used to encrypt the image and division of the encrypted image is done using Random Number. Unless the secret key is known, the original image will not be decrypted. Here secret key ensures the security of images. The proposed method introduces the concept of above scheme. Encryption process encrypts Original Image using variable length Symmetric key, gives encrypted image. Share generation process divides the encrypted images into n number of shares using random number. Decryption process stacks k number of shares out of n to reconstruct encrypted image and uses the same key for decryption.

III. PROPOSED ALGORITHM

Secret sharing schemes protect the secrecy and integrity of information by distributing the information over different locations. The *(t, n)* threshold secret sharing schemes were introduced by Shamir and Blakley independently in 1979 for protecting the cryptographic keys. Generation of shares and reconstruction of shares are challenging task in cheaters scenario. Cheaters identification is critical task on the time of share reconstruction. In this dissertation we proposed a roust secret share generation technique such technique based on cyclic point intersection of langrage's interpolation. In the process of share generation, construction and cheater identification, we proposed four steps. (i) Cyclic share generation (ii) share reconstruction and (iii) cheater identification. The proposed scheme used some notations are defined we assume that P is a participant set that contain n participant p1, p2, p3…………….pn. Such that p= {p1,p2,p3,………….pn} and c1,c2 …cn are cyclic prefix of interpolation equation. Each member of P shares a secret K and hold a secret cyclic prefix Ci where 1≤i≤n.

Share generation phase.

Assume that a dealer wants to share a secret K among the n members in P. First, the dealer specifies the threshold value t freely within the range 1 ≤ t ≤ n. then dealer select three point of prime in subsequent in cyclic x ,y, z .

The dealer randomly generates n different polynomials fi's of degree t−1, such that

$$Fi(X) = a(i,0) + a(i,1)X + \cdots \dots \dots \dots \dots + a(i,t-1)Xt - 1$$

Now then the cyclic point of intersection put into each generated shares Xc, Yc and Zc
As
Consider two distinct points J and K such that J = (xcJ, ycJ) and K = (xcK, ycK)
Let L = J + K where L = (xcL, ycL), then
xcL = s2 - xcJ – xcK
yL = -yJ + s (xJ – xL)
s = (yJ – yK)/(xJ – xK), s is the slope of the line through J and K.
If K = -J i.e. K = (xJ, -yJ) then J + K = O. where O is the point at infinity.
If K = J then J + K = 2J then point doubling equations are used.

Then dealers send the all generated shares to participant.

The Secret Reconstruction Phase
Assume that the participants P1, P2. Pr of any qualified subset in P wants to Cooperate to reconstruct the shared secret K. They can perform the following steps To determine the shared secret K. In the reconstruction phase we apply cyclic addition point of interpolation.

Consider a point J such that J = (xcJ, ycJ), where yJ $\neq$ 0
Let L = 2J where L = (xcL, ycL), Then
xcL = s2 – 2xJ mod p
ycL = -ycJ + s(xcJ - xcL) modZc
s = (3xcJ 2 + a) / (2yJ) mod Zc, s is the tangent at point J and a is one of the parameters
chosen with the elliptic curve. If yJ = 0 then 2J = O, where O is the point at infinity.

IV. EXPERIMENTAL RESULT ANALYSIS

For the validation of proposed method for visual cryptography used mat lab software and some standard attack to measure the security strength of generated share. The result analysis of Digital Image Watermarking based on various image based on two methods. RCVC and Proposed method apply on Barbara image. And we perform White Noise Attack, Gaussian Noise Attack, JPEG Compression Attack, Transform Attack, Cropping Attack, Decoding Attack and find the value of PSNR and NC.

Digital Image	Method of Watermarking	Types of Attack	PSNR	NC
BARBARA IMAGE	RCVC	1.WhiteNoise Attack	50.1575	0.9975
		2.Guassian Noise Attack	70.9659	0.9782
		3.JPEG Compression Attack	40.5286	1
		4.Trasform Attack	42.52168	0.8702
		5.Cropping Attack	44.5189	0.4709
		6.Decoding Attack	36.2288	1
	PROPOSED	1.WhiteNoise Attack	54.3587	0.9997
		2.Guassian Noise Attack	32.4181	1
		3.JPEG Compression Attack	34.5272	1
		4.Trasform Attack	45.5164	0.8702
		5.Cropping Attack	39.5193	0.3857
		6.Decoding Attack	48.0246	1

Table 1 shows the comparative PSNR and NC for Barbara image on the basis of two methods RCVC and proposed method.

Digital Image	Method of Watermarking	Types of Attack	PSNR	NC
Historical Image	RCVC	1.WhiteNoise Attack	65.5584	0.9996
		2.Guassian Noise Attack	81.7818	0.9993
		3.JPEG Compression Attack	22.3644	1
		4.Trasform Attack	32.359	0.8346
		5.Cropping Attack	42.3627	0.3848
		6.Decoding Attack	51.7591	1
	PROPOSED	1.WhiteNoise Attack	86.0932	1
		2.Guassian Noise Attack	70.8216	0.9785
		3.JPEG Compression Attack	42.3641	1
		4.Trasform Attack	32.3589	0.8346
		5.Cropping Attack	52.3631	0.4828
		6.Decoding Attack	66.1775	1

Table 2 shows the comparative PSNR and NC for Historical image on the basis of two methods RCVC and proposed method.

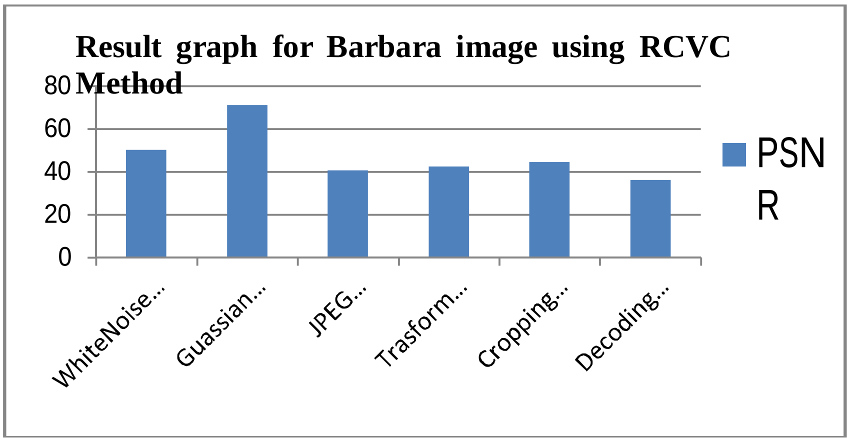

Figure 1: Shows that the Result for Barbara image using RCVC methods, here we find the value of PSNR for their respective types of attacks.

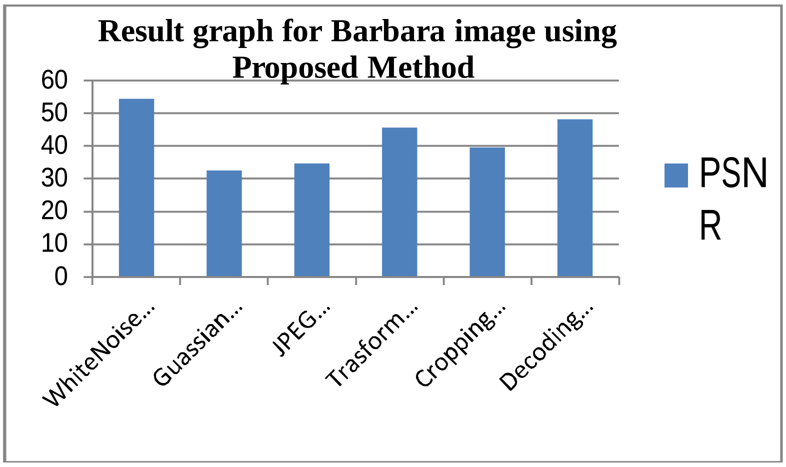

Figure 2: Shows that the Result for Barbara image using Proposed methods, here we find the value of PSNR for their respective types of attacks.

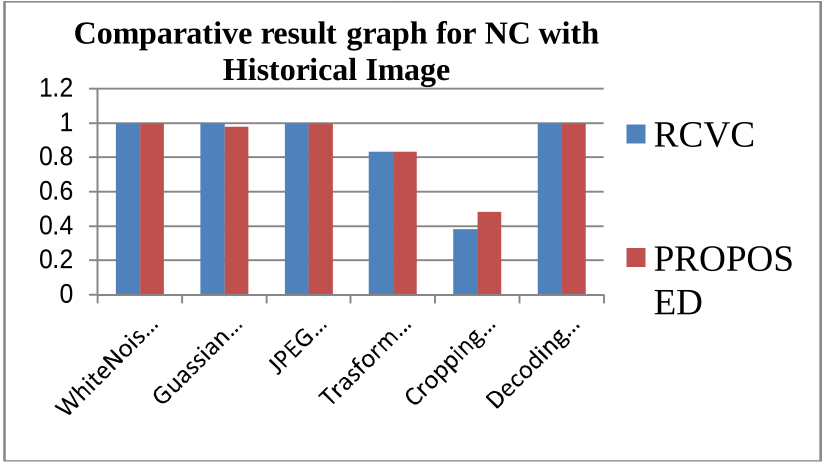

Figure 3: Shows that the comparative result for Historical image using RCVC and Proposed methods, here we find the value of NC for their respective types of attacks.

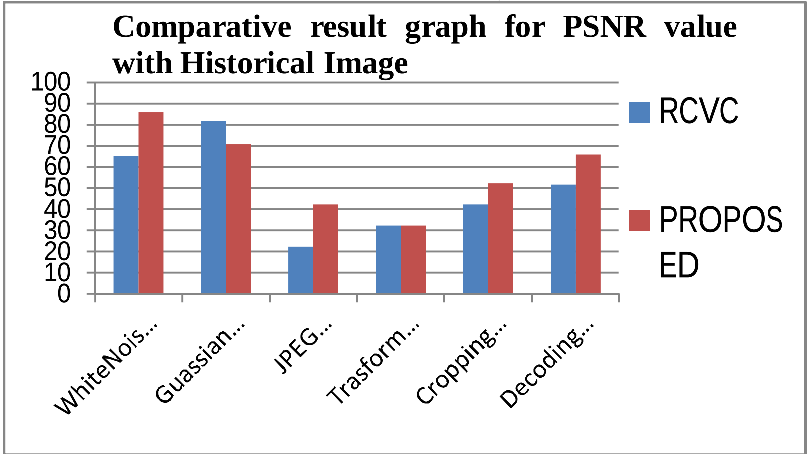

Figure 4: Shows that the comparative result for Historical image using RCVC and Proposed methods, here we find the value of PSNR for their respective types of attacks.

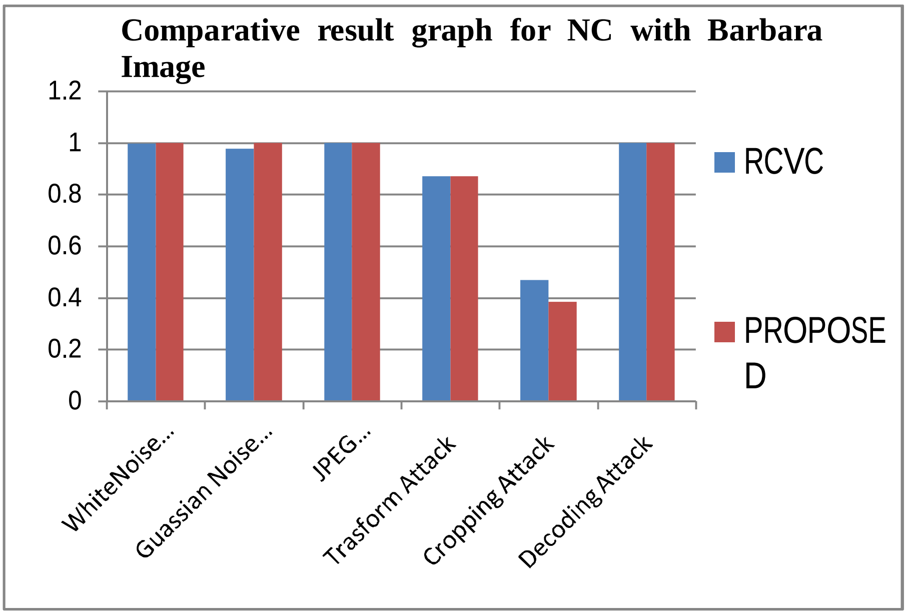

Figure 5: Shows that the comparative result for Barbara image using RCVC and Proposed methods, here we find the value of NC for their respective types of attacks.

V. CONCLUSION & FUTURE SCOPE

In this paper presents the novel methods for visual cryptography based on watermarking technique. the visual cryptography plays a major role in share generation. The process of share generation used for the process of server and OTP authentication. The proposed methods used watermarking technique for the generation of share. The generated share is strength is very high. For penetration and validation used some geometrical attack. The give geometrical attacks not penetrate the proposed system. Our experimental result shows better security strength than pervious algorithm.

REFERENCES

[1] Young-Chang Hou, Shih-Chieh Wei, and Chia-Yin Lin "Random-grid-based Visual Cryptography Schemes" IEEE, 2013, Pp 1-12.
[2] Kai-Hui Lee and Pei-Ling Chiu "Sharing Visual Secrets in Single Image Random Dot Stereograms" IEEE, 2014, Pp 4336-4348.
[3] Xiaotian Wu, DuanhaoOu, Lu Dai, Wei Sun "XOR-Based Meaningful Visual Secret Sharing by Generalized Random Grids" IH&MMSec, 2013, Pp 181-191.
[4] Gayathri Soman, Mr. Jyothish K John "Secure Digital Image Sharing Using Diverse Image Media" IJIACS, 2015, Pp 154-161.
[5] Amitava Nag, Sushanta Biswas, Debasree Sarkar, ParthaPratimSarka, Pp 98-113
[6] Juby Justin and Giss George "An ExtentedVesual Cryptography algorithm for general Access Structures", ijaret, 2013, Pp 1-4.
[7] Anran Wang, Shuai Ma, Chunming Hu, JinpengHuai, Chunyi Peng, Guobin Shen "Enhancing Reliability to Boost the Throughput over Screen-Camera Links", IEEE, 2013, Pp 1-12.
[8] Bharanivendhan N and Amitha T "Visual Cryptography Schemes for Secret Image Sharing using GAS Algorithm", International Journal of Computer Applications, 2014, Pp 11-16.
[9] Jun Kong, Omer Barkol, Ruth Bergman, AyeletPnueli, Sagi Schein, Kang Zhang, and Chunying Zhao "Web Interface Interpretation Using Graph Grammars" IEEE, 2012, Pp 590-602.
[10] Sian-Jheng Lin, Shang-Kuan Chen and Ja-Chen Lin "Flip visual cryptography (FVC) with perfect security, conditionally-optimal contrast, and no expansion", Elsevier, 2010, Pp 900-916.
[11] Wazir Zada Khan,Yang Xiang, Mohammed Y Aalsalem, Quratulain Arshad "Mobile Phone Sensing Systems: A Survey", IEEE, 2013, Pp 402-427.
[12] J. Galbally "Biometric Antispoofing Methods: A Survey in Face Recognition", IEEE, 2015, Pp 1530-1552.
[13] Snehal N. Meshram and Sneha U. Bohra "Implementation of Random Grid Visual Cryptography for Color Images", IJSR, 2013, Pp 2545-2549.