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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

A Competent and Speedy Symmetric Key Production with improved Latency Using Matrix Array Symmetric Key Encryption

Brajesh Kumar [1], Santosh Kumar[2]

Assistant Professor, Department of Computer Science & Engineering, Women's Institute of Technology, Darbhanga, Bihar, India[1]

Assistant Professor, Department of Computer Science & Engineering, Women's Institute of Technology, Darbhanga, Bihar, India[2]

ABSTRACT: Share generation play an important role in text cryptography and visual cryptography. The generation of share prevents 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, Decipherment, Joint Key Cryptography, Secret Sharing, Public key Cryptography.

I. INTRODUCTION

The concept of visual cryptography was first proposed by Naor and Shamir [9] in 1994. Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by humans (without computers). It involved breaking up the image into n shares so that only someone with all n shares could decrypt the image by overlaying each of the shares over each other. Practically, this can be done by printing each share on a separate transparency and then placing all of the transparencies on top of each other. In their technique n-1 shares reveals no information about the original image.

Visual crypto-graphic scheme for a set P of n participants is a cryptographic paradigm that enables a secret image to be split into n shadow images called shares, where each participant in P receives one share. Certain qualified subsets of participants can "visually" recover the secret image with some loss of contrast, but other forbidden sets of participants have no information about the secret image. A large number of cryptography algorithms have been created till date with the primary objective of converting information into unreadable ciphers (an encrypted piece of text).

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

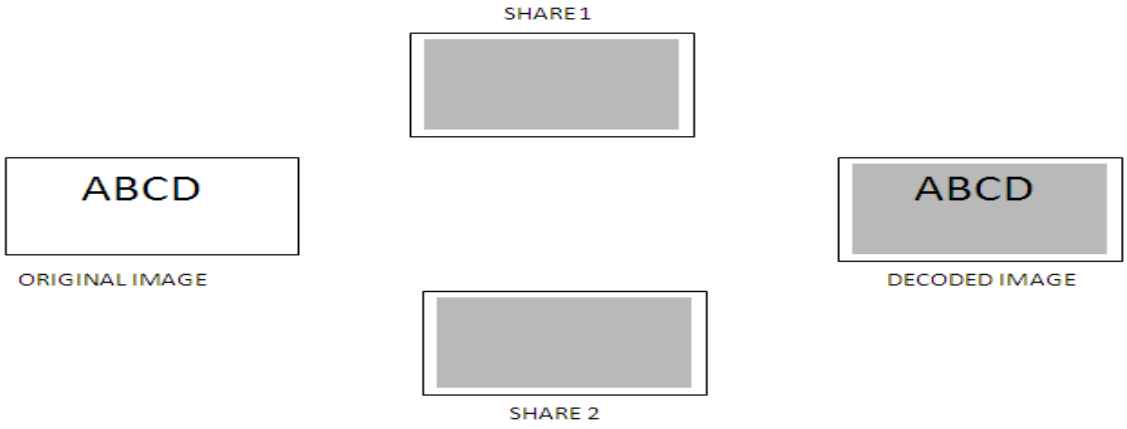

Figure 1: Working of visual cryptography.

Although visual cryptography has become a focus of research in the field of secret image protection, there are still some practicality problems left unsolved. For one thing, the camouflage image must be printed on transparencies so that the transparencies can be stacked together to reveal the secret image. However, it is usually not a very convenient thing to carry transparencies around. If the camouflage images were printed on paper or stored in the cell phone, then it would not cause too much trouble.

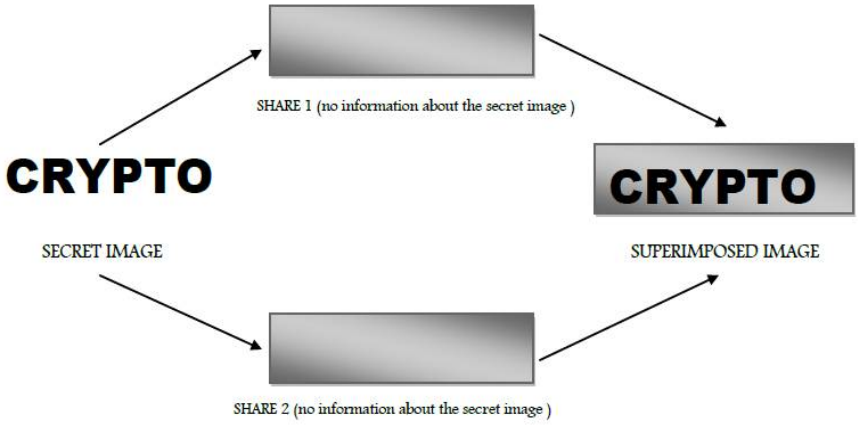

Figure 2. (2, 2)-VTS for black and white image.

1.1 THE JOINT KEY CRYPTOGRAPHY

The joint key cryptography (Symmetric key cipher) uses a common key for encryption and decryption of the message. This key is shared privately by the sender and the receiver. The sender encrypts the data using the joint key and then sends it to the receiver who decrypts the data using the same key to retrieve the original message. Joint key cipher algorithms are less complex and execute faster as compared to other forms of cryptography but have an additional need to securely share the key. In this type of cryptography the security of data is equal to the security of the key. In other words it serves the purpose of hiding a smaller key instead of the huge chunk of message data.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

1.2 THE PUBLIC KEY CRYPTOGRAPHY

The public key cryptography (asymmetric key cipher) is a technique that uses a different key for encryption as the one used for decryption. Public key systems require each user to have two keys a public key and a private key (secret key). The sender of the data encrypts the message using the receiver's public key. The receiver then decrypts this message using his private key. This technique eliminates the need to privately share a key as in case of symmetric key cipher. Asymmetric cryptography is comparatively slower but more secure than symmetric cryptography technique. The public key cryptography is a fundamental and most widely used technique, and is the approach which underlies Internet standards such as Transport Layer Security (TLS) (successor to SSL). The most common algorithm used for secret key systems is the Data Encryption Algorithm (DEA) defined by the Data Encryption Standard (DES). A HYBRID CRYPTOSYSTEM is a more complex cryptography system that combines the features of both joint and public key cryptography techniques.

1.3 VISUAL DECIPHERMENT

Decipherment is the art of hiding the existence of the communication message before sending it to the receiver. It has been practiced since 440 B.C. in many ways like writing information on the back of cattle in a herd, invisible ink etc. Some relatively modern ways include hiding the information in newspaper articles and magazines etc. Multimedia Decipherment is one of the most recent and secures forms of Decipherment. It started in 1985 with the advent of the personal computer applied to classical Decipherment problems. Visual Decipherment is the most widely practiced form of Decipherment and is usually done using image files. It started with concealing messages within the lowest bits of noisy images or sound files. Images in various formats like jpeg have wide color spectrum and hence do not reflect much distortion on embedding data into them.

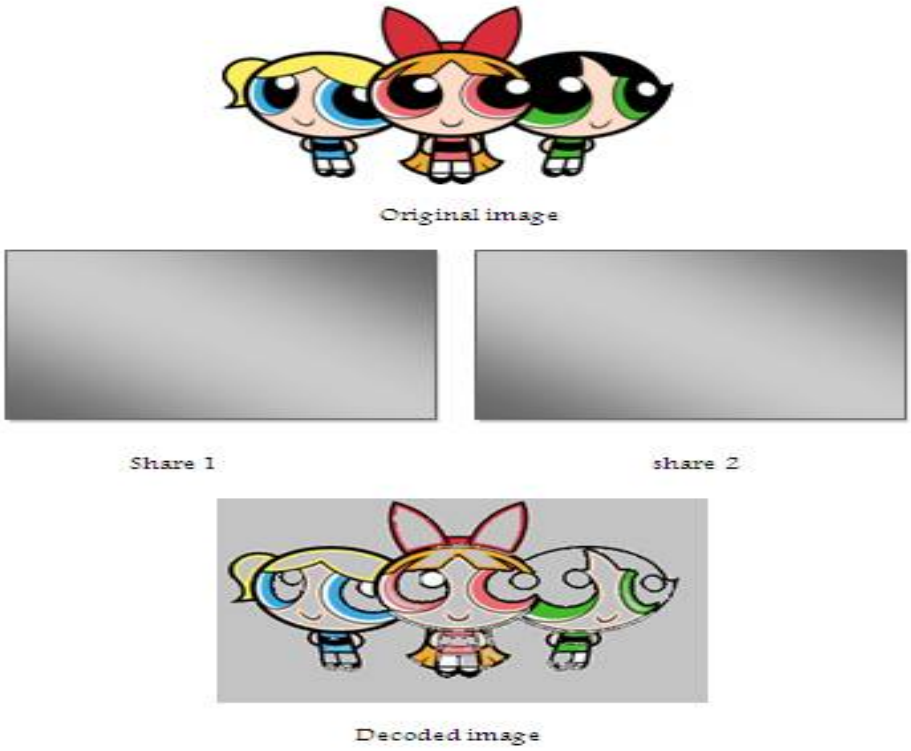

Figure 3: Example of Visual Cryptography.

1.4 SECRET SHARING

Secret sharing allows sharing secret information among a group of participants such that decoding is possible only when all the participants are present with their shares. Secret can be divided into any number shares. A part of secret

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

information is called a share. While decoding the information, it is required to take all the shares on transparency and then superimpose them in proper order. There are various secret sharing schemes. Among all available, the author concentrated on 2 out of 2 secret sharing schemes. 2 out of 2 secret sharing schemes divide secret information into exactly 2 shares. When these two shares are observed separately, no one can reveal the secret information. Among two shares, one acts as a cipher text and other acts as secret key. However, by carefully aligning the transparencies , the original secret message is reproduced. While generating shares, each pixel in original is represented as a group of pixel in shares. We used 4X4 pixel matrix in shares to represent a single pixel. Encoding of original can be done using horizontal pixels, vertical pixels or diagonal pixels. We used random combination of these types while encoding. Figure 3 represents the model of visual cryptography and represents the possible shares for original black pixel. In visual cryptography the revealed image is the expansion of original image. Every pixel in original image is replaced by a pixel matrix of 2X2 hence expanded version of the picture. There is existence of distortion after decryption. The model for 2 out of 2 secret sharing schemes, Share 1 and share 2 are generated in such a way that the pixel present 1 share is not present on another share. Upon superimposing these shares, the original image is revealed.

1.5 VISUAL SECRET SHARING SCHEME

In the encryption step, a secret image is read as input. After the encryption, two noise-like share images with pixel expansion will be produced. These two shares are higgledy-piggledy and meaningless by human eye. They have interlaced structure with black and white pixels. The length and width of these share images are enlarged 2 times that of the secret image. In the decryption process, we can easily get the secret information by stacking two share images. When the pixel of secret image is white, the corresponding pixels of stacking image will be indicated by the gray-level-like black and white cross points. Otherwise When the pixel of secret image is black, the corresponding pixels of stacking image will be structured by all black pixels. Therefore, after stacking two share images, we can clearly recognize the secret information by the human eye. Owing to the length and width of share images are extend twice that of the secret image, pixels in the share image have been extended to four times pixels as that of the secret image.

II. RELATED WORK

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by humans without the aid of computers. The following section provides an introduction to visual secret sharing scheme, halftone visual cryptography and error diffusion techniques.

2.1 PiyushMarwaha ,PareshMarwaha[1] “Visual Cryptographic Decipherment In Images” in this title author describe Cryptography involves converting a message text into an unreadable cipher. On the other hand, Decipherment embeds message into a cover media and hides its existence. Both these techniques provide some security of data neither of them alone is secure enough for sharing information over an unsecure communication channel and are vulnerable to intruder attacks. Although these techniques are often combined together to achieve higher levels of security but still there is a need of a highly secure system to transfer information over any communication media minimizing the threat of intrusion.

In this paper we propose an advanced system of encrypting data that combines the features of cryptography, Decipherment along with multimedia data hiding. This system will be more secure than any other these techniques alone and also as compared to Decipherment and cryptography combined systems. Visual Decipherment is one of the most secure forms of Decipherment available today. It is most commonly implemented in image files. However embedding data into image changes its colour frequencies in a predictable way. This method can be used to increase the security on web based applications. The user will be asked to provide the secret key and the password can be compared from image files using the key. It can be used as advancement over the existing option to input the security phrase in various web based applications.

2.2 Young-Chang Hou and Zen-Yu Quan [2] “Progressive Visual Cryptography with Unexpanded Shares” In this letter, we proposed a brand new sharing scheme of progressive VC to produce pixel-unexpanded shares. In our research, the possibility for either black or white pixels of the secret image to appear as black pixels on the shares is the same, which approximates to 1/n. Therefore, no one can obtain any hidden information from a single share, hence

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

ensures the security. When superimposing k (sheets of share), the possibility for the white pixels being stacked into black pixels remains 1/n, while the possibility rises to k/n for the black pixels, which sharpens the contrast of the stacked image and the hidden information, therefore, become more and more obvious. After superimposing all of the shares, the contrast rises to (n − 1)/n which is apparently better than the traditional ways that can only obtain 50% of contrast, consequently, a clearer recovered image can be achieved.
In the traditional VSS scheme, the secret is transformed into n shares of noise-like images. The original secret can be visually obtained only when a subset of at least k shares are available and are well stacked together. This is an advantage in the situation if no computer is available. However, the (k, n)-threshold sharing scheme is an all-or-nothing method, which means that the secret image can be reconstructed if at least k of n shares are available, but with less than k shares nothing of the secret will be revealed on the stacked image. Besides, even if we have shares more than the threshold value k, the secret information would not be revealed more than it.

2.3 Ching-Lin Wang, Ching-Te Wang, Meng-Lin Chiang "The Image Multiple Secret Sharing Schemes Without Pixel Expansion" [3] In this paper, two secret sharing schemes were proposed. The two schemes both have the characteristic that the share images they produced are with no pixel expansion. In encoding phase, the rotated share scheme creates two share images for hiding three secret images, whereas the Exclusive OR rotated scheme achieve three share images for hiding four secret images. In decoding phase, the first scheme get secret information by stacking images and rotating image with different angles (0°, 90°, 180°). The second scheme get secret information by doing XOR operation, stacking, and rotating image with different angles (0°, 90°, 180°, 270°). Compare with other schemes of Visual Cryptography, our schemes not only increase the quantity of secret information, but also enhance quality of share image without increasing embed data.
Base on share image without pixel expansion, we proposed two image secret sharing schemes. The first scheme uses two share images to hiding three secret information images, while our second scheme uses three share images to hiding four secret information images. By using rotating image and matching block method, the second scheme increase more hiding secret information images. The experiment results show that our two schemes can easily preserve the share images also the stacking secret information image can be seen clearly. In the design of hiding secret share image, we increase more capacity of hiding by using mathematical operation and not increase the burden of hiding process. That is a strong point for secret information sharing transmission and security.

2.4 Debasish Jena, Sanjay Kumar Jena "A Novel Visual Cryptography Scheme" [4] in this title author describe Visual Cryptography is a new cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by human, without any decryption algorithm. Here we propose a Data hiding in halftone images using conjugate ordered dithering (DHCOD) algorithm which is a modified version of Data hiding in halftone images using conjugate error diffusion technique (DHCED). We use this DHOCD algorithm for proposing a new three phase visual cryptography scheme. DHCOD technique is used to hide a binary visual pattern in two or more ordered dither halftone images, which can be from the same or different multi-tone images. In proposed scheme we shall generate the shares using basic visual cryptography model and then embed them into a cover image using a DHCOD technique, so that the shares will be more secure and meaningful.
Visual cryptography is the current area of research where lots of scope exists. Currently this particular cryptographic technique is being used by several countries for secretly transfer of hand written documents, financial documents, text images, internet voting etc. There are many possible enhancements and extensions exist of the basic visual cryptographic model introduced till now. One such enhancement we are trying to do. There are other areas also in visual cryptography which are still open where no satisfactory results yet achieved as colour visual cryptography, enhancement of image shares with respect to contrast, size, quality and clarity of revealed image. Researchers are still busy for finding the new application where visual cryptography can be used.

2.5 Thomas Monoth, BabuAnto P "Contrast-Enhanced Visual Cryptography Schemes Based on Additional Pixel Patterns" [5] in this title author describe Visual cryptography is a kind of secret image sharing scheme that uses the human visual system to perform the decryption computations. A visual cryptography scheme allows confidential messages to be encrypted into k-out-of-n secret sharing schemes. Whenever the number of participants from the group (n) is larger than or equal to the predetermined threshold value (k), the confidential message can be obtained by these

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

participants. Contrast is one of the most important parameters in visual cryptography schemes. Usually, the reconstructed secret image will be darker (through contrast degradation) than the original secret image. The proposed scheme achieves better contrast and reduces the noise in the reconstructed secret image without any computational complexity. In this method, additional pixel patterns are used to improve the contrast of the reconstructed secret image. By using additional pixel patterns for the white pixels, the contrast of the reconstructed secret image can be improved than in the case of existing visual cryptography schemes.

2.6 Pallavi Vijay Chavan, R.S. Mangrulkar "Encrypting Informative Color Image using Color Visual Cryptography" [6] in this title author describe Color Visual Cryptography scheme implemented in this paper encrypts informative color image in such a way that result of encryption is in the form of shares. Shares do not reflect any information directly, information is scrambled instead. Each share carries some information which in unreadable by necked eyes. The decryption is done directly by the human visual system with no special cryptographic calculations. Color visual cryptography uses 2 out of two secret sharing scheme which generates two shares for every input image to be encrypted. The original image is reconstructed by printing the two output shares onto transparencies and superimposing them together. This is X-OR operation between the shares to reveal the original information. The algorithm first generates RED, GREEN, BLUE as well as the ALPHA components of each pixel of an input image and these three components are used to generate the shares using 2 out of 2 secret sharing scheme.

2.7 Nitty Sarah Alex, L. JaniAnbarasi "Enhanced Image Secret Sharing via Error Diffusion in Halftone Visual Cryptography" [7] in this title author describe Visual Cryptography is an encryption technique where a secret image is cryptographically encoded into n shares. In visual secret sharing scheme (k,n) the secret images can be visually revealed by stacking together any k or more transparencies of the shares and by inspecting less than k shares one cannot retrieve the secret image. Visual Secret Sharing based on halftone visual cryptography, the continuous-tone image is first transformed into a halftone image, and then encrypted using visual secret sharing schemes. In visual cryptography, meaningless shares are encoded into halftone shares taking meaningful visual information which reduces the suspicion of intruders. These halftone shares are concurrently error diffused to give visually pleasing effect. Error diffusion is computationally efficient with less complexity. Techniques such as classical fixed, edge enhancement, green noise and block error diffusion are performed and a comparative study is made. The quality of the halftone shares enhanced by using Floyd - Steinberg and Jarvis error filters. Secret image is reconstructed by stacking the qualified halftone shares.

In this paper various techniques of error diffusion is applied to improve the image quality of the halftone shares. The halftoning visual cryptographic method inserts the secret information pixels into preexisting un-coded halftone shares. Visual cryptography is used along with the concept of halftoning where the continuous-tone image is first transformed into a binary image, and then the visual secret sharing is applied. The secret image is encoded into halftone shares taking meaningful visual information by concurrently using error diffusion to halftone shares. Error diffusion has low complexity and provides halftone shares with good image quality. A reconstructed secret image, obtained by stacking qualified shares together, does not suffer from cross interference of share images.

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.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

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 $1 \leq t \leq n$. 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
- $Fi(X) = a(i,0) + a(i,1)X + \cdots \ldots \ldots \ldots + a(i,t-1)Xt - 1$
- 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.

Cheaters detection phase:

In the cheater detection phase, reconstructed shares find the point of intersection of cyclic in langrage's interpolation the difference value of cyclic prefix is 0 there is no cheater and the cyclic point generate a difference 1 then there is cheater.

IV. EXPECTED OUTCOMES

In This Proposal Design an Efficient Secret Share Generation Technique Using Visual Cryptography and langrage's interpolation equation. The proposed method divide into two sections one is share generation and another is cheater detection. Some expected outcomes in the proposed method.

1. Reduces the time of share generation
2. Maintain the length of share equal to key size
3. Detect the cheater who generate the fake share
4. Increase the time of intentional attack
5. Signing key with a TPS concept

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

REFERENCES

1. PiyushMarwaha, PareshMarwaha "Visual Cryptographic Decipherment In Images" International conference on Computing, Communication and Networking Technologies, IEEE, 2010. Pp 1-6.
2. Young-Chang Hou and Zen-Yu Quan "Progressive Visual Cryptography with Unexpanded Shares" IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, Vol-21, 2011. Pp 1760-1764.
3. Ching-Lin Wang, Ching-Te Wang, Meng-Lin Chiang "The Image Multiple Secret Sharing Schemes Without Pixel Expansion" International Conference on Machine Learning and Cybernetics, IEEE, 2011. Pp 1838-1844.
4. Debasish Jena, Sanjay Kumar Jena "A Novel Visual Cryptography Scheme" International Conference on Advanced Computer Control, IEEE 2007. Pp 208-213.
5. Thomas Monoth, BabuAnto P "Contrast-Enhanced Visual Cryptography Schemes Based on Additional Pixel Patterns" International Conference on Cyberworlds, IEEE, 2010. Pp 171-177.
6. Pallavi Vijay Chavan, R.S. Mangrulkar "Encrypting Informative Color Image using Color Visual Cryptography" Third International Conference on Emerging Trends in Engineering and Technology, IEEE 2010. Pp 277-283.
7. Nitty Sarah Alex, L. JaniAnbarasi "Enhanced Image Secret Sharing via Error Diffusion in Halftone Visual Cryptography" IEEE, 2011. Pp 393-397.
8. F. Liu1, C.K. Wu1 X.J. Lin "Colour visual cryptography schemes" Published in IET Information Security, Vol-2, 2008. Pp 151-164.
9. Xiaotian Wu, Wei Sun "A Novel Bit Plane based Image Sharing Scheme using EVCS" International Conference on Information, Networking and Automation, IEEE 2010. Pp 540-544.
10. L. JaniAnbarasi, M. Jenila Vincent, G.S. Anandha Mala "A Novel Visual Secret Sharing Scheme for Multiple Secrets via Error Diffusion in Halftone Visual Cryptography" International Conference on Recent Trends in Information Technology, IEEE 2011. Pp 305-309.