Visual Cryptography in the Video using Halftone Technique

Bhawna Shrivas
M.Tech Scholar
Mahakal Institute of Technology
Behind Air Strip, Dewas Road,
Ujjain (M.P.)-456664, India

Shweta Yadav
Reader
Mahakal Institute of Technology
Behind Air Strip, Dewas Road,
Ujjain (M.P.)-456664, India

ABSTRACT
The image cryptography is one of the techniques used in the data security during communication over public domain. In the many researchers are working to make the visual cryptography techniques more robust and secure against the attack. In this paper, we have proposed the visual cryptography in the video with the halftone image as a secrete image. We have used Floyd and Jarvis technique for halftoning. The comparative results of PSNR and RMSE has been given in paper for these two techniques.

Keywords
Halftone, Embedding, PSNR, RMSE etc.

1. INTRODUCTION
The Image security is a very vast field of the application of image processing in the data security system. The visual cryptography is one of the technique used to transmit the secrete image under the cover image. Visual cryptography is invented by Moni Neor and Adi Shamir in 1994. A visual cryptography is related with the Human vision systems. Initially black and white image is used as a secrete image.

Now a days the gray image is used as a secrete image using a technique called digital half toning .The half toning is the lossy process and it is impossible to recover the secrete image as it is original image. The block diagram is showing the process of cryptography [1].

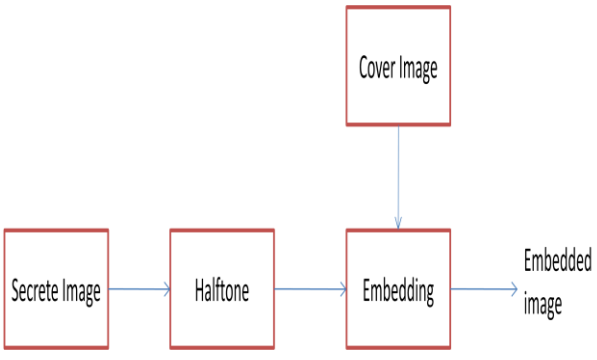

Fig 1: Process of cryptography

Visual cryptography allows effective and efficient secret sharing between a numbers of trusted parties. With many cryptographic schemes, for trust is the most difficult part. In the visual cryptography provides a very powerful technique by which one secret can be distributed into two or more shares. The shares are Xeroxed onto transparencies and then superimposed exactly together; in original secret can be discovered without computer participation.

Many applications based on visual cryptography have been developed. [2]. A multiparty scheme is presented for co-owners of digital image. Many novel algorithms have been proposed in the fields of Steganography and visual cryptography with the goals of improving reliability, security, and efficiency George et.al [3] have compares the two methodologies and proposed a possible algorithm which combines the use of both steganography and visual cryptography.

Young et al. [4] have proposed a intellectual property protection scheme for digital images based on visual cryptography and statistical property. The result of comparing two pixels that are selected randomly from the host image determines the content of the master share. Their method does not need to alter the original image and can identify the ownership without restoring to the original image. In besides, their method allows multiple watermarks to be registered for a single host image without causing any damage to other hidden watermarks. Moreover, it is also possible for this scheme to cast a larger watermark into a smaller host .

The importance of utilizing biometrics to establish personal authenticity and to detect imposters is growing concern in the present scenario of global. The visual cryptographic methods can be used to detract the suspicious looking peoples. In [5] authors have proposed secure tongue biometric authentication system using visual cryptography.

In this paper we have used Jarvis and Floyd technique for half toning and its effect on the received image is presented.

2. LITERATURE REVIEW
Naor and Shamir's [6] have proposed a (k, n) threshold visual cryptography scheme which encodes a given secret image into n shadow images process, where any k or more of them can visually recover the secret image, but any k-1 or fewer of them fail to recover the secret image. It exploits the human visual system to read the secret message from some overlapping shares function, these overcoming the disadvantage of complex computation required in the traditional cryptography.

In [7] Wu et al have proposed a visual cryptography schemes to share two secret images in two shares. In the hidden two secret binary images into two random Shares, for namely A and B, such that the first secret can be seen by stacking the two shares.

In [8] S J Shyu et al authors have proposed the multiple secrets sharing in visual cryptography. This scheme encodes a set of $n \geq 2$ secrets into two circles. The n secrets can be obtained one by one by stacking the first share and the rotated

second shares with n different rotation angles this system image. In this scheme two secret images which are encoded into two shares; one secret image appears with just stacking two shares and the other secret image appears with stack two shares after reversing one of them. Another Jen-Bang Feng et al [9] developed a visual secret sharing scheme for hiding multiple secret images into two shares. the embedded data can be extracted with some procedure process. On the other hand, visual cryptographic techniques break up a secret image into several shares so that only someone with all shares can decrypt the secret image by superposing all shares together They embed secret image data into several halftone images without affecting their perceptual qualities and the embedded data can be restored with apparently high quality when the halftone images are overlaid without any special electronic calculation.

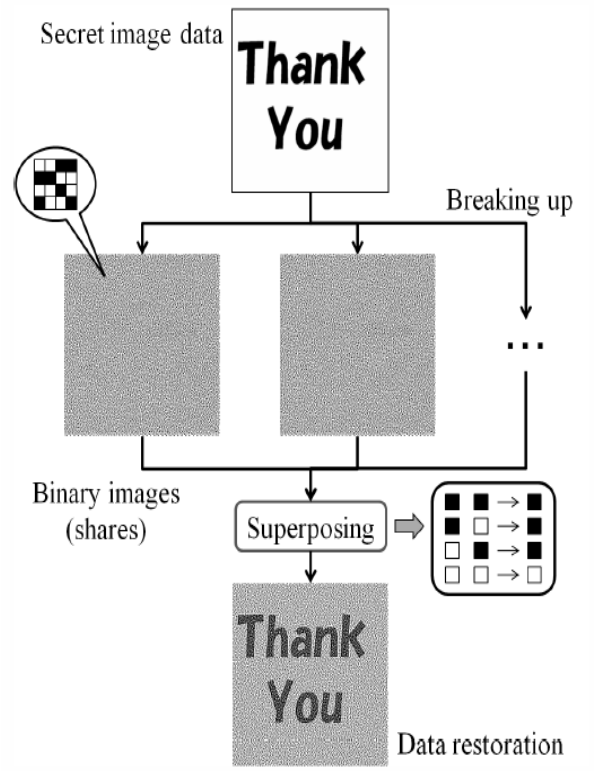

Fig 2: Typical flow chart of visual cryptography scheme.

Visual cryptography encodes a secret binary image into shares of random binary pattern. If the secret image can be visually decoded by superimposing a qualified subset of transparencies, no secret information can be obtained from the superposition of a forbidden subset process. In [10] authors have proposed a novel technique named halftone visual cryptography. Based on the blue-noise dithering principles, their proposed method utilizes the void and cluster algorithm to encode a secret binary image into halftone shares (images) carrying significant visual information source. Their simulation shows that the visual quality of the obtained halftone shares is observably better than that attained by available visual cryptography method.

In [11] Conventional visual cryptography methods divide a secret digital image into n pieces and distribute them to n participants. This paper proposes a novel approach to visual cryptography for binary images that includes the capabilities of watermarking and verification image. The proposed method allows an n×n watermark image to be embedded into an n×n secret image to construct two shadows and then to be used to verify the accuracy of the reconstructed image. The checking to determine the reliability of all shadows before they are used to recover the secret image prevents a participant from incidentally or deliberately providing invalid data.

Gopi et. al [12] have proposed a new cryptography scheme for securing color image based on visual cryptography. In a color image to be protected and a binary image used as key to encrypt and decrypt are taken as input data. A secret color image which needs to be communicated is decomposed into three monochromatic images based on YCbCr color space system. Then these monochromatic images are converted into binary image, in the finally the obtained binary images are encrypted using binary key image, in a called as share-l to obtain binary cipher images. To encrypt Exclusive OR operation is done between binary key image and three half-tones of secret color image separately.

In [13], a verifiable visual cryptography scheme is proposed to verify whether the share is authorized, in which authors have introduced a Third Trusted Party (TTP) whose action is guaranteed. A simulation result shows that the visual quality of the obtained halftone share is observably better [14]. A novel (2, m+1) visual cryptographic technique has been proposed image data, where m number of secret images has been encrypted based on a randomly generated master as a common share for all secrets which is decodable with any of the shares in conjunction with master share out of m + 1 generated shares.

In [16], authors introduces the concept of visual information pixel (VIP) synchronization and error diffusion to attain a color visual cryptography encryption method that produces meaningful color shares with high visual quality. The visual information pixel (VIP) synchronization retains the positions of pixels carrying visual information of original images throughout the color channels and error diffusion generates shares pleasant to human eyes. For the Comparisons with previous approaches show the superior performance of the new method.

3. METHODOLOGY

Proposed solution performs visual cryptography for videos. The steps can be understood at transmitter end and receiver end separately.

Steps at transmitter end:

- Read Input Secure Video and splited into frames, each frame is now become a color image.
- Now each frame is decomposed into three monochromatic images based on RGB color space.
- The halftoning technique is applied to these monochromatic images to reprography them into binary images. Halftoning: is the process of transforming an image with greater amplitude resolution to one with lesser amplitude resolution.
- Read the share image or key image.
- Now XOR operation is performed between binary images obtained in halftone process and share 1/key image separately.
- Repeat this process for every binary image in the video.

- Now splitted binary image are again merged to form a video. This video is now hide behind the share image such as when we play the video only share image will be display. No one can recognize the video

Steps performed at Receiver side:

- Read the encrypted video.
- Split the video into frames.
- For each frame perform the following :
- Split the frame into RGB.
- De-embedd the share image and each binary secrete image of video/frame.
- Inverse halftoning is performed on each image.

4. RESULT

The PSNR and RMSE of the embedded and receive image are the key factor has been considered for the performance evolution. Higher PSNR at embedded image become limitation of the getting higher PSNR of received image.

The frame of the secrete video has been shown in figure below:

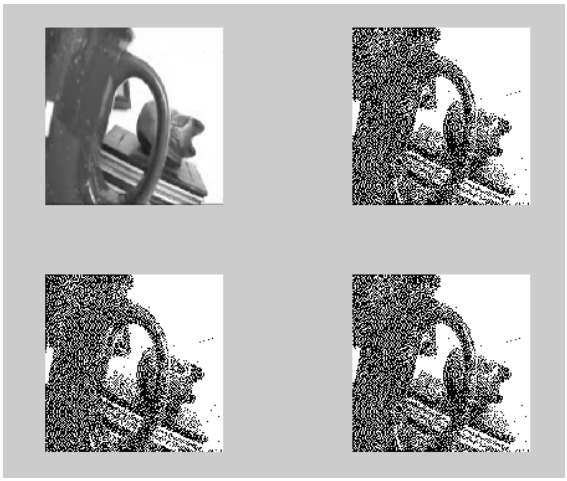

Fig 3: frame of the secrete video and its color component.

The cover image for cryptography is shown in figure below

Fig 4: Frame of the cover image.

The embedded and recovered frames are given as figure below

Fig 5: Embedded and recovered frames.

Comparison table for two methods are shown below. Table for 20 frames are shown:

PSNR			RMSE	
Jarvis	**Floyd's**		**Jarvis**	**Floyd's**
13.28981	14.9970565		55.214084	45.361494
11.93287	13.4274658		64.550083	54.345913
13.15377	14.0359797		56.08561	50.668867
13.09769	13.9109499		56.44895	51.403499
13.08209	13.9104632		56.550382	51.40638
13.09836	13.9159346		56.444555	51.374008
13.10015	13.9180676		56.432928	51.361394
13.10066	13.9305852		56.429656	51.287428
13.08921	13.9465233		56.504088	51.193405
13.06545	13.9303838		56.658848	51.288617

The 50 video frames has been encrypted and transmitted with both the method halftoning techniques, The PSNR result for this two method are given as below:

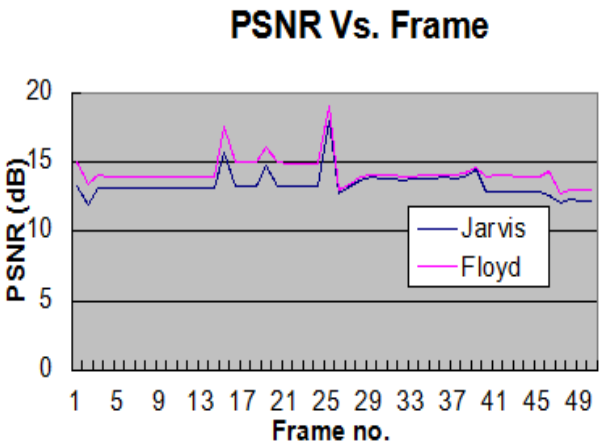

Fig 6: PSNR of received video with Jarvis and Floyd halftone method

The RMSE of the received video is as follows.

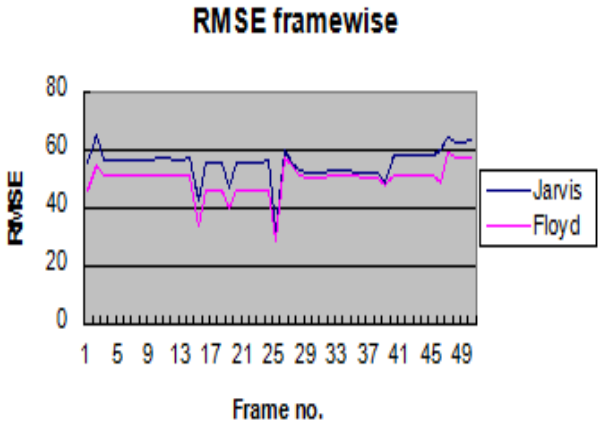

Fig 7: RMSE of received video with Jarvis and Floyd halftone method

5. CONCLUSION

Visual cryptography in the video with the halftone image as a secrete image has been developed and simulated in this paper. Floyd and Jarvis technique are used for half toning before the encryption. The effect of the methods as results of PSNR and RMSE has been given and found Floyd has performed better than Jarvis halftone method

6. FUTURE WORK

Further extend this work to use this technique by creating 8 shares of secret image. It is also possible that secret video can be hidden behind any audio or video. Future work can also reduce the computational time taken by video to convert into frames

7. ACKNOWLEDGMENTS

Our thanks to the experts who have contributed towards development of the template.

8. REFERENCES

[1] Visual Cryptography and Its Applications, Jonathan Weir, WeiQi Yan, BookBoon 2012

[2] Shen Ying," Visual Cryptography based Multiparty Copyright Protect Scheme", 978-1-4244-5848-6/10/ ©2010 IEEE

[3] George Abboud, Jeffrey Marean, Roman V. Yampolskiy," 2010 Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering", 978-0-7695-4052-8/10 © 2010 IEEE DOI 10.1109/SADFE.2010.14

[4] Young-Chang Hou, Pei-Hsiu Huang," Image protection based on visual cryptography and statistical property", 2011 IEEE Statistical Signal Processing workshop (SSP)

[5] Sowmya Suryadevara, Rohaila Naaz, Shweta, Shuchita Kapoor, Anand Sharma," Visual Cryptography Improvises the Security of Tongue as a Biometric in Banking System", International Conference on Computer & Communication Technology (ICCCT)-2011, 978-1-4577-1386-611@2011 IEEE

[6] M.Naor, A. Shamir, "Visual cryptography,"Advances in Cryptology-EUROCRYPT'94, LNCS, vol.950,pp.1-10,1995.

[7] C.C. Wu, L.H. Chen, "A Study On Visual Cryptography", Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998.

[8] S.J.Shyu, S.Y.Huanga, Y.K.Lee, R.Z.Wang, and K.Chen, "Sharing multiple secrets in visual cryptography", Pattern Recognition, Vol.40, Issue 12, pp.3633-3651,2007.

[9] Wen-Pinn Fang, "Visual Cryptography In Reversible Style", IEEE Proceedingon the Third International Conference on Intelligent Information Hidingand Multimedia Signal Processing (IIHMSP2007), Kaohsiung, Taiwan, R.O.C,2007

[10] Zhi Zhou, Member,Gonzalo R. Arce, Giovanni Di Crescenzo, "Halftone Visual Cryptography", IEEE transactions on image processing, vol. 15, no. 8, august 2006

[11] Zhi-hui Wang, Chin-Chen Chang, Huynh Ngoc Tu, "Sharing a Secret Image in Binary Images with Verification" Journal of Information Hiding and Multimedia Signal Processing Volume 2, Number 1, January 2011

[12] Gopi Krishnan S and Loganathan D,"Color Image Cryptography Scheme Based on Visual Cryptography ",Proceedings of 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011)

[13] Han Yanyan, Cheng Xiaoni, Yao Dong, He Wencai," VVCS: Verifiable Visual Cryptography Scheme", 2011 Seventh International Conference on Computational Intelligence and Security

[14] Nitty Sarah Alex, L. Jani Anbarasi," Enhanced Image Secret Sharing via Error Diffusion in Halftone Visual Cryptography".

[15] J. K. Mandal, Subhankar Ghatak, "A Novel Technique for Secret Communication through Optimal Shares using Visual Cryptography (SCOSVC)", 2011 International Symposium on Electronic System Design.

[16] InKoo Kang, Gonzalo R. Arce, Heung-Kyu Lee, " Color Extended Visual Cryptography Using Error Diffusion", IEEE transactions on image processing, vol. 20, no. 1, january 2011