Video Encryption by Using Visual Cryptography Based on Wang's Scheme

Rinaldi Munir
School of Electrical Engineering and Informatics
Institut Teknologi Bandung
Bandung, Indonesia
rinaldi.munir@itb.ac.id

Harlili
School of Electrical Engineering and Informatics
Institut Teknologi Bandung
Bandung, Indonesia
harlili@itb.ac.id

***Abstract*—Visual cryptography could be used to encrypt secret video so that each participant has their own share in encrypted form. The encrypted video could be played. To recover the original video, all participants have to join their shares. In this paper, we developed a method to encrypt video by using Wang's scheme. If the secret video has the audio, then the scheme is applied to each frame. The audio could be combined to each share or not. Experiment results show that the scheme could be applied very well to video. The recovered video is same exactly with the original video.**

Keywords—visual cryptography, video, Wang's scheme.

I. INTRODUCTION

Digital information can be represented in different types. In computer information can be represented through text, audio, video, and animation. Video is a kind of audio visual information that contains frames of image and audio (if any), therefore a video has richer information than a single image. Video can be transmitted and stored easily. However, with rapid development of information technology, security and privacy issues of video are very important today. An authorized party could access a private video that has sensitive data. Solution of the problem is by encrypting it. Data encryption is a suitable method to protect the video from an authorized access. Video in encrypted form couldn't be read by an authorized party without knowing the key(s) to decrypt it into the original video. Cryptography is art and science to encrypt the message. Any conventional encryption algorithm such as DES, Blowfish, AES, RC4, RSA, etc, actually coud be applied to encrypt video. Furthermore, there are some algorithms that are specifically used for video encryption such as VEA, MVEA, and RVEA. An overview of video encryption techniques can be found in [1]. Since the video has a large volume of data, selective encryption techniques are used to reduce encryption and decryption time, so that the techniques could be applied for real time video encryption [2].

The video encryption mentioned above usually is used for one-to-one communication. For example, Alice send a video to Bob. Before Alice transmit it, Alice encrypt the video with the secret key. Bob receive a encrypted video from Alice, Bob has to decrypt it with the same secret key before enjoy the video. Futhermore, there is another problem to share the encrypted videos to some participants, but to decrypt the video, part or all participants have to join their shares in order to reconstruct the original video. Solution of this problem is by using visual cryptography technique. Concept of visual cryptography firstly was published in 1994 by Naor and Shamir [3]. This concept is called the secret image sharing scheme. A secret image is encrypted by encoding the image into some transparencies or *shares*. Decyption of the image is very simple because only use the human visual system. The original image is reconstructed by stacking the shares and information is read visually. A short survey of visual cryptography techniques and applications can be found in [4].

Visual cryptography could be applied to any multimedia data such as image, video, and audio. Solanki et al. in [5] proposed a system to encrypt and decrypt multimedia files (documents, images, audio, video) using AES (Advanced Encryption Standard) and visual cryptography. In the system, the multimedia file must be converted first to be a text file using Base64 encoding. Next, the encrypted file is encoded using a visual cryptography technique. Therefore, if the input is a video file, then the output is some image shares, not some videos.

Different to [5], Shrivas and Yadav in [6] proposed the visual cryptography to hide the secret video into the cover video using the halftone technique. Each frame of video decomposed into three monochromatic images based on RGB color space. The halftoning technique is applied to these monochromatic images to result binary images, and performing XOR operation between the binary images with the key. Next, the three binary image are again merged to form a video. Therefore, the video is hide behind the share images.

In this paper, we propose a method to encrypt video using a secret sharing scheme. The video may be contain audio or not. If the video contains audio, only frames of video will be encrypted. The video is splitted into *n* shares, each participant gets a share. To reconstruct the original video, all shares must be combined using XOR operation. The secret sharing scheme is based on Wang's scheme [7] and technique to process frames of video is based on [8]. Size of frames of shared video are equal to original frames and the original frames reconstructed perfectly (from *n* shares of the participants) without loss of contrast.

The paper is organized into five sections. The first section is this introduction. The second section will review some related works about visual cryptography. The method to encrypt video using visual cryptography will be explained in the third section. The fourth section will discuss the experiment results. The last section will resume the conclusion and future works.

II. RELATED WORKS

A. Visual Cryptography

Concept of visual cryptography firsty is introduced by Naor and Shamir in 1994. Encryption process needs

computation, but decryption process is without computation, it is easily done by human visual system. They proposed a simple scheme for binary images. Each pixel in a binary images is subdivided into a set of m black and white subpixels in each of n shares for n participants, every participant get a share. Fig. 1 illustratea a scheme with $m = 2$ and $n = 2$, it is called as 2-out-of-2 scheme or (2, 2) scheme.

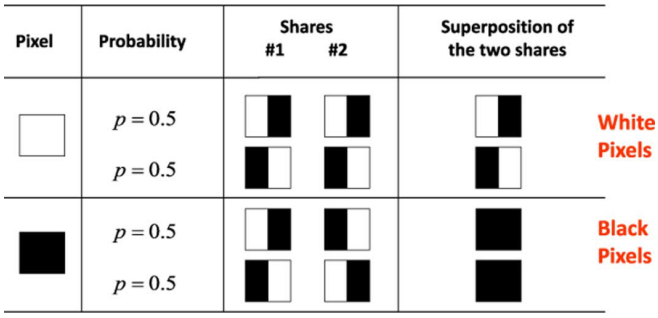

Fig. 1 Illustration of a 2-out-of-2 scheme with 2 subpixel construction [8]

To read the message in the original binary image, two shares are stacked together, and human visual system will perceive the reconstructed pixel as "black" or "white". Fig. 2 shows the secret image ('drum'), two shares, and reconstructed image as stacking result. The reconstructed image appears to contain noises.

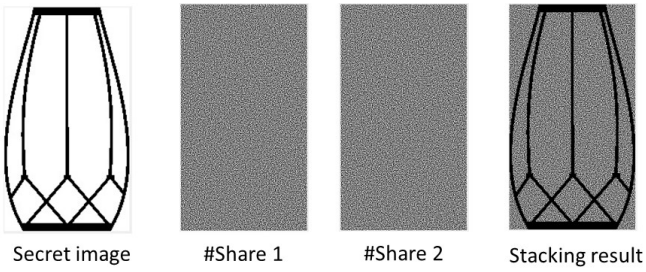

Fig. 2 Example of Naor and Shamir's visual cryptography scheme

Some researchers developed more visual cryptography schemes so that applied to grayscale and color secret images [9, 10].

B. *Wang's Secret Color Image Sharing Schemes*

Unfortunately, all of secret image sharing schemes expand one pixel into multiple sub-pixels. As the consequence, size of shared images increase. For example, if one pixel is expanded into four subpixels, then size of the shared images increase four times. In addition, the reconstructed image is not same exactly with the original image, it is loss of contrast and contains noises that make it looks like a noisy image [11]. In 2005, Wang et all proposed a (n, n) secret image sharing scheme based on XOR operation without pixel expansion and results better contrast [7]. The (n, n) scheme means that one image will be shared to n shares, each for one participant, and to recover the original image, n participants have to join their shares. The secret image can be reconstructed perfectly by using XOR operation. The scheme is applied to grayscale and color images.

Wang's scheme is very simple. Assume that the original image of size $M \times N$ pixels is represented as matrix $A = [a_{ij}]$, a_{ij} represents graylevel of the pixel, $a_{ij} \in \{0, 1, ..., c-1\}$, c is maximum of graylevel, $i = 1, 2, \ldots, M$, and $j = 1, 2, \ldots, N$. Suppose that the shared images are $A_1, A_2, \ldots, A_n$. Algorithm of the (n, n) scheme can be resumed as follows.

Firstly, generate $n-1$ random matrix $B_1, B_2, \ldots, B_{n-1}$ of the same size as matrix A. Matrix $B_k = [b_{ij}]$ where $b_{ij} \in \{0, 1, ..., c-1\}$. The shares are produced as a sequence of XOR operation:

$$\begin{aligned} A_1 &= B_1 \\ A_2 &= B_1 \oplus B_2 \\ &\ldots \\ A_{n-1} &= B_{n-2} \oplus B_{n-1} \\ A_n &= B_{n-1} \oplus A \end{aligned} \quad (1)$$

To reconstruct the image, XOR-ing all the shares as follows:

$$A_1 \oplus A_2 \oplus A_3 \oplus ... \oplus A_{n-1} \oplus A_n = A \quad (2)$$

Equation (2) could be explained as follows:

$$\begin{aligned} &A_1 \oplus A_2 \oplus A_3 \oplus ... \oplus A_{n-1} \oplus A_n = \\ &B_1 \oplus (B_1 \oplus B_2) \oplus (B_2 \oplus B_3) \oplus ... \oplus (B_{n-2} \oplus B_{n-1}) \oplus B_{n-1} \oplus A = \\ &(B_1 \oplus B_1) \oplus (B_2 \oplus B_2) \oplus (B_3 \oplus ... \oplus B_{n-2} \oplus (B_{n-1} \oplus B_{n-1}) \oplus A = \\ &(0 \oplus 0 \oplus \ldots \oplus 0) \oplus A = 0 \oplus A = A \end{aligned}$$

Therefore, the original can be recovered again. Fig. 3 shows experiment results of the (4, 4) scheme to image of birds (450 × 299) [11]. There are four shares with the same size as the original image. By XOR-ing all shares we will recover the original image exactly.

(a) Secret image (b) share #1

(c) Share #2 (d) Share #3

(e) Share #4 (d) Reconstructed image

Fig. 3 Results of applying (4, 4) threshold scheme [11]

III. METHOD

Suppose Alice has a secret video. She wants to share the encrypted videos to three participants: Bob, Carol, and Eve, but to recover the original video, all participants have to combine their shares. The (3, 3) secret sharing scheme based on Wang's scheme will be used to solve this problem. Fig. 4 shows this problem.

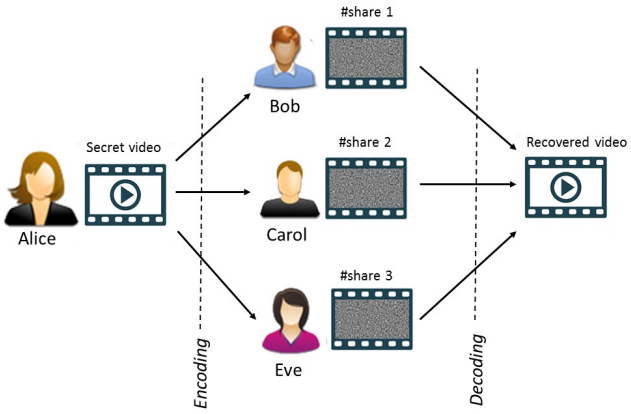

Fig. 4 Video secret sharing scheme based on Wang's scheme

The video has many frames, therefore we have to perform the Wang's scheme for each frame independently. Because of a frame has three color channels (*R*, *G*, and *B*), therefore the Wang's scheme is applied to each color channel.

The method is divided to two phases, encoding and decoding. In encoding phase, a secret video will be encoded to *n* video shares, whereas in decoding phase, *n* video shares will be decoded to reconstruct the original video.

A. Encoding

Asume that there are *m* frames (A_1, A_2, …, A_m) and *n* participants, therefore in order to apply the Wang's scheme we have to generate $m \times (n-1)$ random matrix B_{k_i} ($k = 1, 2, \ldots, m$; $i = 1, 2, \ldots, n-1$). Every set of B_{k_i} will be used to produce *n* shares A_{k_i} of each frame A_i. Each frame A_k will produce *n* shares. Every share with number *i* ($i = 1, 2, \ldots, n$) of frame *k* ($k = 1, 2, \ldots, m$) is combined to produce a video share *i*. The Wang's scheme will be as follows:

$$\begin{aligned} A_{k_1} &= B_{k_1} \\ A_{k_2} &= B_{k_2} \oplus B_{k_2} \\ &\vdots \\ A_{k_n} &= B_{k_{n-1}} \oplus A_k \end{aligned} \tag{3}$$

for $k = 1, 2, \ldots, m$. The shared video for *n* participants are as follows:

The first video share: $\{A_{1_1}, A_{2_1}, \ldots, A_{k_1}\}$

The second video share: $\{A_{1_2}, A_{2_2}, \ldots, A_{k_2}\}$

…

The n^{th} video share: $\{A_{1_n}, A_{2_n}, \ldots, A_{k_n}\}$

Now each participant has their own share. The shared video could be played, but in encrypted video. Each participant couldn't decrypt their share without combined to other shares.

B. Decoding

To recover the original video, all participants combine their shares by XOR-ing all the shares of each frame *i* to recover frame *i* as follows:

$$A_{k_1} \oplus A_{k_2} \oplus \ldots \oplus A_{k_n} = A_k \tag{4}$$

for $k = 1, 2, \ldots, m$. Combine all frames to recover the original video.

C. Flowcharts

Fig. 5 shows flowchart of encoding phase to produce the shares of video. The secret video may be contain the audio. If the video has an audio layer, audio data will be separated from its video, and Wang's scheme will be applied to all frames. Also, if the secret video contains the audio, user could choose if the shared videos will be combined with the audio or not. Each video shares will be have same audio. The audio itself usually is not encrypted. Output of the encoding phase are *n* video shares.

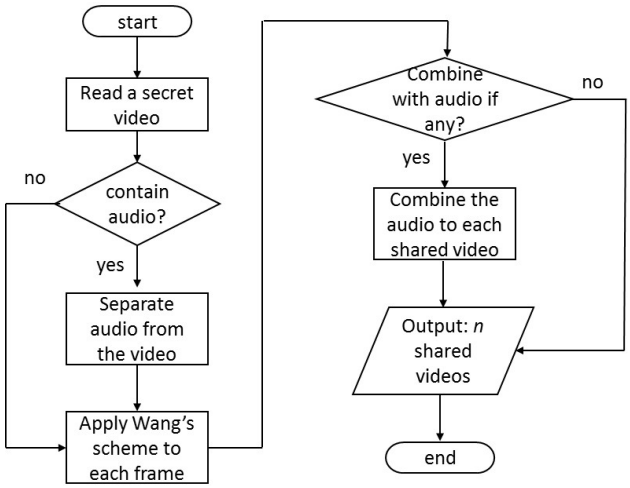

Fig. 5 Flowchart of encoding phase

Fig. 6 shows flowchart of decoding phase to recover the original video. Input of this phase are all video shares. Similarly, if video shares have an audio layer, the audio data will be separated from its video. Each corresponding frame of each video share will be XOR-ed to recover the original frame. If the video shares contain audio, then combine the audio with the recovered frames to yield the original video.

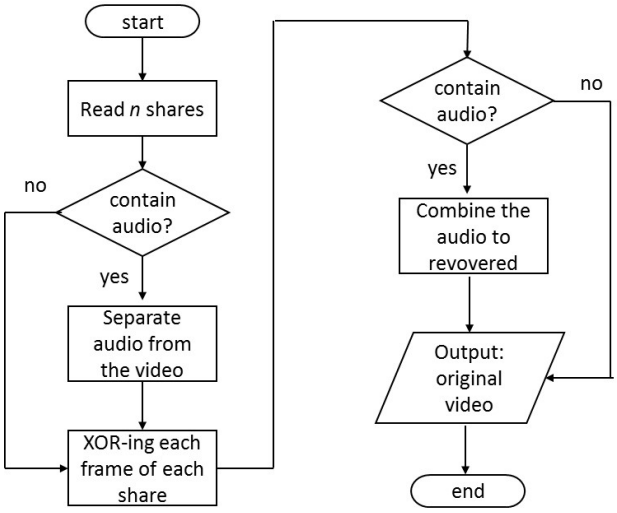

Fig. 6 Flowchart of decoding phase

IV. Experiment and Results

The method above has been implemented into computer program and tested to some sample videos. We used two kinds of videos. First kind, video without audio, video has frames only. The second kind, video that contains audio. For both kinds of videos, only frames of video is encrypted using Wang's scheme, whereas the audio is not encrypted. Program could receive video files in any format (AVI, MPG, MP4, etc.), however the output videos (shared videos and recovered video) are in AVI format only. Four test video are shown in Fig. 7, whereas properties of each video (duration, number of frames, and audio layer) is shown in Table 1.

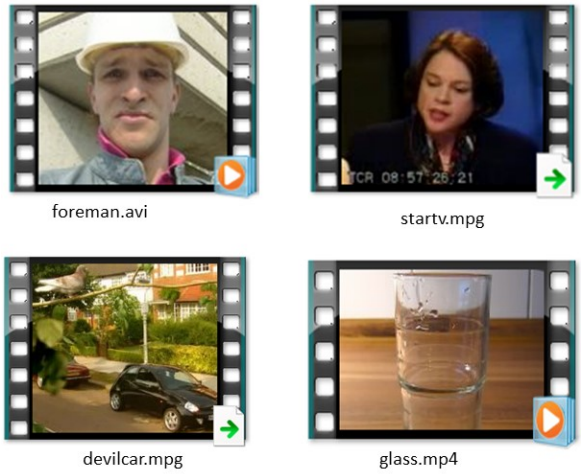

Fig. 7 Four test videos in variety formats

Table 1. Properties of test videos

No.	Video	Duration (s)	Number of frames	Frame size	Has Audio?
1	Foreman.avi	33.3	400	144x176	No
2	Devilcar.mpg	23	576	240x320	Yes
3	StartTV.mpg	93.3	2793	112x176	Yes
4	Glass.mp4	10	240	480x854	Yes

For all experiments, we used (3, 3) scheme of Wang. It means that one secret video will be shared to three video shares, each for every participant, and to reconstruct (or recover) the original video three participants have to join their video. If less than three, then the original video could not be recovered.

In the Wang's scheme no key needed to encoding (encrypt) video. It's true that to generate random matrices (B_{k_i}) required a seed, but the seed does not required anymore in decoding (decryption) phase, because decoding process doesn't use the matrices. Because of all participants have to join their shares, therefore one of the shares will behave as a key.

In our experiment we encoded each of the test videos become to three shares, and to then we joined the three shares to reconstruct the original video. We also measured encoding time and decoding time. In next experiment we tried to decode the original video using less than three shares.

A. Results

All of test video could be encoded into three shares, and from the three shares we could reconstruct the original videos in AVI format. In this page we show only screenshots of folder that contain the original video `foreman.avi` and `glass.mp4`, three shares of the videos, and the reconstructed videos (`foreman-out.avi` and `glass-out.avi`) (see Fig. 8 and Fig. 9).

Fig. 8 Experiment results of video `foreman.avi`. (a) Original video; (b), (c), and (d) are shares; (e) reconstructed video

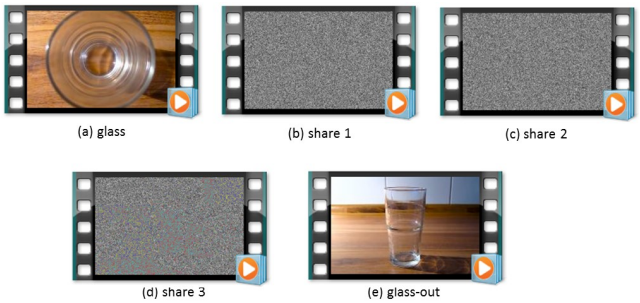

Fig. 9 Experiment results of video `glass.mp4`. (a) Original video; (b), (c), and (d) are shares; (e) reconstructed video

Table 2 shows duration time of encoding (encryption) and decoding (decryption) of all test videos. The duration is not included time for reading and writing video files. We measured only time to generate of random matrices, time to generate the shares, and time to reconstruct the original video. Execution of program is performed three times and then we calculate the average.

Table 2. Duration of encoding and decoding

No.	Video	Encoding (second)	Decoding (second)	Number of frames	Frame size
1	Foreman.avi	1.38808	0.067731	400	144x176
2	Devilcar.mpg	5.362532	0.241483	576	240x320
3	StartTV.mpg	10.22913	0.402041	2793	112x176
4	Glass.mp4	23.28912	0.648802	240	480x854

Fig. 10 shows some frames of foreman video and the frames of the shares. The frames displayed here are frame number 10, 200, 280, and 375. All of frames of the the shares are in encrypted form.

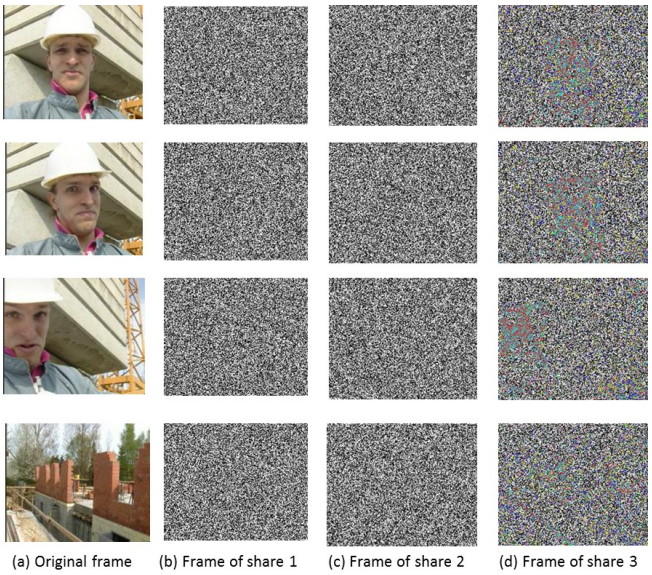

Fig. 10 Some frames of original foreman video and frames of the shares (from top to bottom: frame number 10, 200, 280, 375).

What happened if we recover the original video from any two shares? The original video is failed to reconstruct. Fig. 11 shows three cases.

- Case 1, participant 2 and participant 3 join their shares.
- Case 2, participant 1 and participant 2 join their shares.
- Case 3, participant 1 and participant 3 join their shares.

However, the original video couldn't be recovered in all cases.

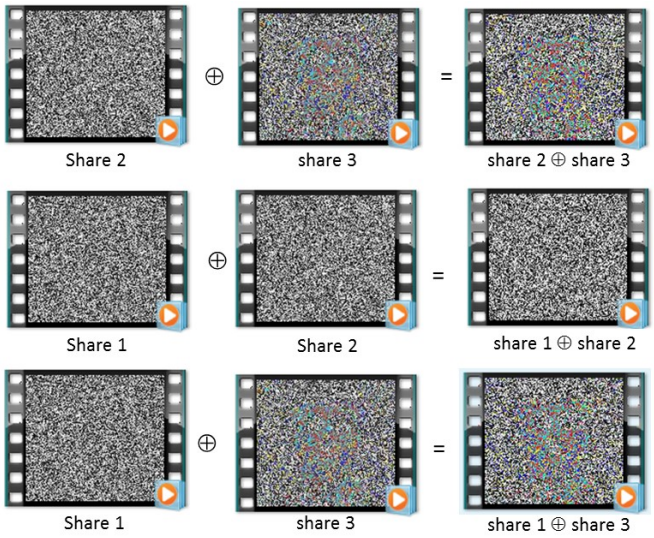

Fig. 11 The original video is failed to reconstruct if two participants join their shares

B. *Discussion*

We have performed experiments to ensure that the method worked well. All videos could be encoded to some shares in encrypted form. The original videos could be reconstructed again exactly from the shares.

Encoding and decoding time depend on number of frames and frame size. The more the number of frames, the longer the encoding time. Likewise, the larger the frame size, the longer the encoding time. Video `glass.mp4` has the highest encoding time, because the frame size is large compared to other videos. Interestingly, decoding time is very fast compared to encoding time, because the decoding process is XOR operation between the shares only. To reduce encoding time, alternatively we could perform the Wang's scheme in another color model, for example in *YCbCr* color model. We apply the Wang's scheme to *Y* component, whereas to *Cb* and *Cr* components we enough perform XOR operation with a random matrix. However, this alternative is complicated and need additional time to transform from RGB to YCbCr and vice versa.

Another experiment also proved that the original video is failed to reconstruct when number of shares is less than *n*. The Wang's scheme is (*n*, *n*) threshold scheme, it means that to reconstruct the original video we need *n* shares.

V. Conclusion and Future Works

The (*n, n*) threshold scheme of Wang scheme could be used as a method to share the encrypted video to *n* participants. To reconstruct the secret video, all shares of the participants has to be combined together. The secret video may be have the audio and user could choose if the shares will contain audio or not. Experiment results show that the scheme could be applied very well to encrypt video. The recovered video is same exactly with the original video

Acknowledgment

This paper is fully funded by the P3MI ITB batch year 2018.

REFERENCES

[1] M. Abomhara, O. Zakaria, O. O. Khalifa, "An Overview of Video Encryption Techniques", *International Journal of Computer Theory and Engineering*, Vol. 2, No. 1 February, 2010.

[2] A.A. Ramdan, R. Munir, Selective Encryption Algorithm Implementation for Video Call on Skype Client, Proceeding of 2012 7th International Conference on Telecommunication Systems, Services, and Applications (TSSA).

[3] M. Naor and A. Shamir, "Visual cryptography". Advances in Cryptology EUROCRYPT '94. Lecture Notes in Computer Science, (950):1–12, 1995

[4] H. Abdolrahimpour, E. Shahab, "A Short Survey of Visual Cryptography and Secret Image Sharing Techniques and Applications", International Advanced Research Journal in Science, Engineering and Technology, Vol. 4, Issue 3, March 2017

[5] K. Solanki, V. Vankani, P. Pukle, S. Iyer, "Multimedia Encryption Using Visual Cryptography", *International Journal of Recent Trends in Engineering & Research (IJRTER)*, Vol. 02, Issue 09; September - 2016

[6] B. Shrivas, S. Yadav, "Visual Cryptography in the Video using Halftone Technique", *International Journal of Computer Applications* (0975 – 8887), Vol.117 – No.14, May 2015

[7] D. Wang, L. Zhang, N. Ma, L. Huang, "Secret Color Images Sharing Schemes Based on XOR Operation". 2005..

[8] Ross, A., "Visual Cryptography for Biometric Privacy", *IEEE Transaction on Information Forensics and Security*, Vol. 6, No. 1, March 2011.

[9] V. Rijmen and B. Preneel, "Efficient colour visual encryption or 'Shared colors of benetton'," *Eurocrypt' 96 Rumpsession Talk,* ttp://www.esat.kuleuven.ac.be/~rijmen/vc/.

[10] E. Verheul and H. V. Tilborg., Constructions and properties of k out of n visual secret sharing schemes. *Designs, Codes and Cryptography, 11(2):179–196, 1997*.

[11] Munir, R., Comparison of Secret Color Image Sharing Based on XOR Operation in RGB and YCbCr Color Space, Proceeding of ICEEI 2017.