INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

(Volume2, Issue4)

Available online at: www.Ijariit.com

ROBUSTNESS AGAINST SHARP AND BLUR ATTACK IN PROPOSED VISUAL CRYPTOGRAPHY SCHEME

Dhirendra Bagri *
bagri.dhirendra@gmail.com
Computer Engineering and Application, NITTTR Bhopal

R. K. Kapoor
rkkpoor@nitttrbpl.ac.in
Computer Engineering and Application, NITTTR Bhopal

***Abstract*— The fundamental reason of watermarking invention was to protect originality of image message in the first place from outside attack. The quality of image depends on its ability to survive against various kinds of attacks that try to remove or destroy the originality. However, attempting to remove or destroy the message meaning should produce a noticeable debility in image quality. The robustness is a factor that plays an important role to test and verify the algorithm whether it will withstands against these attacks or not. In this paper the robustness of the proposed algorithm [15] for secret image share in Visual Cryptography Scheme is identified. The robustness of the image against various attacks, specifically image blur attack and image sharp attack are tested. The study of calculated PSNR value signifies the proposed algorithm withstands successfully on these attacks.**

***Keywords*— DHCOD, PSNR, MSE, SLSB, Wavelet transform, Cryptographic, Watermarking, revealed image.**

I. INTRODUCTION

Visual Cryptography (VC) is a method of encrypting a secret image into shares such that stacking a sufficient number of shares reveals the secret image. Shares are binary images usually presented in transparencies. Unlike conventional cryptographic methods, VC needs no complicated computation for recovering the secret image. The act of decryption is to simply stack shares and view the secret image that appears on the stacked shares. Visual cryptographic technique is being used by several countries for secretly transfer of images in army, hand written documents, financial documents, text images, internet- voting etc. Watermarking is the technique of embedding a secret image into a cover image without affecting its perceptual quality so that secret image can be revealed by some process. One significant advantage of watermarking is the inseparability of the watermark (secret image) from the cover image. Some of the vital characteristics are: hard to perceive, resists ordinary distortions, endures malevolent attacks, carries numerous bits of information, and demands little computation to insert and extract watermarks. Share generation for the visual cryptography can also be done using watermarking technique. These watermarked shares can be used for retrieving the hidden information.

II. BASIC IDELOGY OF IMAGE SHARE IN VC

The image is represented as the set of pixels. Each component image has a pair of pixels for every pixel in the original image. These pixel pairs are shaded black or white according to the following rule: if the original image pixel was black, the pixel pairs in the component images must be complementary; randomly shade one ■□, and the other □■. When these complementary pairs are overlapped, they will appear dark gray. On the other hand, if the original image pixel was white, the pixel pairs in the component images must match: both ■□ and both □■. When these matching pairs are overlapped, they will appear light gray. So, when the two component images are superimposed, the original image appears. However, considered by it, a component image reveals no information about the original image; it is indistinguishable from a random pattern of ■□ / □■ pairs. Moreover, the particular, figure1 shows that each pixel is broken into two sub pixels. Let B shows black pixel and T shows Transparent (White) pixel. Each share will be taken into different transparencies. When both transparencies are placed on top of each other, the following combinations are received, for black pixel BT+TB=BB or TB+BT=BB and for white pixel BT+BT=BT or TB+TB=TB. Similarly in Figure 2 is given where each pixel is broken into four sub pixels. Likewise, 4C2 =6 is the number that can be different cases for this approach.

1: Each Pixel is broken into two sub pixels as follows.

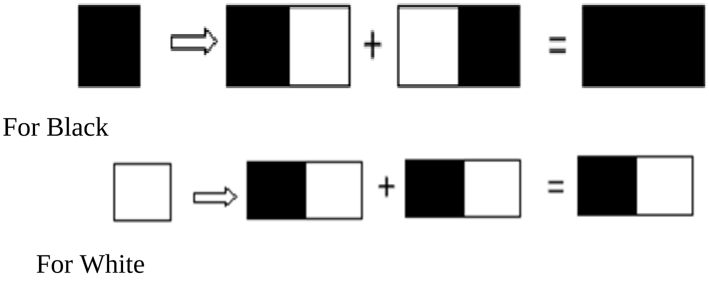


Fig 1 Pixel broken into two sub pixel

2: Each Pixel is broken into four sub pixels as follows.

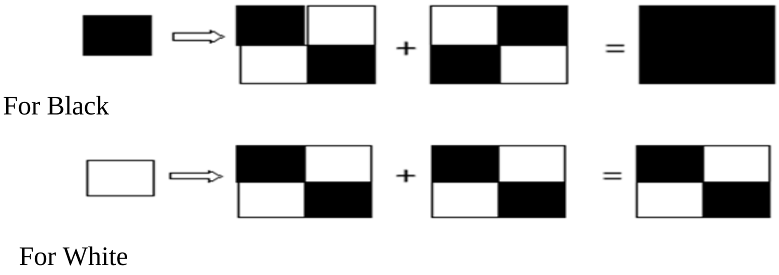


Fig 2 Pixel broken into four sub pixel

III. ROBUSTNESS STUDY IN VARIOUS TEHNIQES

1) DHCOD algorithm [4] was used for generating the shares. A dithered halftone image generated by the cover image has been used as first share. Fig.3 shows the working model of DHCOD algorithm. This scheme also has drawbacks as the visual quality of watermarked image, and the revealed image is not rich.

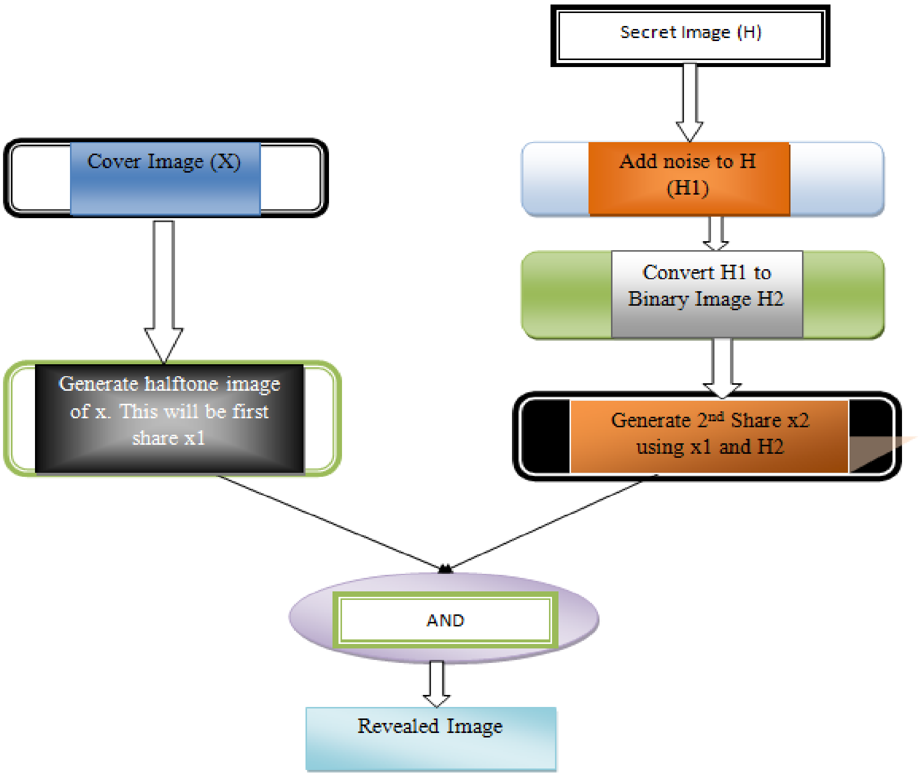

Secret Image (H)
Cover Image (X)
Add noise to H (H1)
Convert H1 to Binary Image H2
Generate halftone image of x. This will be first share x1
Generate 2nd Share x2 using x1 and H2
AND
Revealed Image

Fig 3 Working model of DHCOD algorithm

2) Least Significant Bit Coding (LSB): LSB coding [5] can be applied to any form of watermarking.LSB coding is a very simple technique but the robustness of the watermark will be too low. With LSB coding almost always the watermark cannot be retrieved without a noise component.

3) Predictive Coding Schemes: Predictive coding [6] scheme was proposed by Matsui and Tanaka for grey scale images. This is much more robust when compared to LSB coding.

4) *Patchwork Techniques:* In patchwork watermarking [7], the image is divided into two subsets. One feature or an operation is chosen and it is applied to these two subsets in the opposite direction. For instance if one subset is increased by a factor k, the other subset will be decreased by the same amount. If a[i] is the value of the sample at I in subset ‘A’ which is increased and b*i+ is the value of the sample in the subset ‘B’ whose value is decreased, then the difference between the two subsets would intuitively result in

$$\Sigma\,(a[i]-b[i]) = 2N \text{ for watermarked images} \qquad 1<=N<=\infty$$
$$= 0 \qquad \text{otherwise}$$

4) Wavelet Transform based Watermarking: The Fourier transform [8] is an analysis of global frequency content in the signal. There are applications in digital image processing wherein localized frequency components are needed. This can be done by using the Short Time Fourier Transform. This is similar to the concept of using windowing functions. The windowed transform is given as

$$F(\omega,\alpha) = \int_{-\infty}^{\infty} \mathrm{f(x)g(x-\alpha)\,e^{-j\omega x}dx}$$

Where ‘ω’ denotes the frequency and ‘α’ denotes the position of the window. This equation transforms the signal f(x) in a small window around ‘α ’.The STFT is then performed on the signal and local information is extracted. The wavelet transform based watermarking technique divides the image into four sidebands- a low resolution approximation of the tile component and the component’s horizontal, vertical and diagonal frequency characteristics.

5) Proposed image share technique:

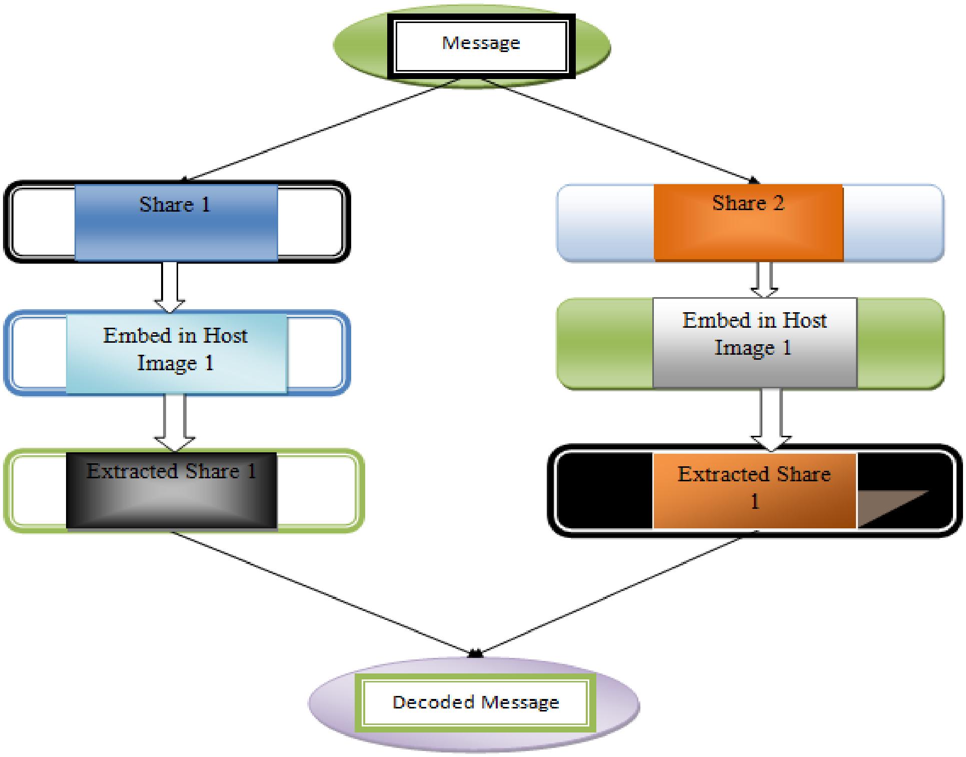


Fig 4 Structure of the Proposed Scheme

The proposed scheme[15] generates the VC shares using basic visual cryptography model and then embed them into a cover image using invisible blind watermarking technique as shown in figure 5.1, so that the secret shares will be more secure, meaningful and shares are protected from the Malicious adversaries who may alter the bit sequences to create the fake shares. During the decryption phase, secret shares are extracted from the respective cover images without using any cover image characteristics to provide mutual authenticationFig.5shows share creation using VC (2, 2) Encryption. When two shares are stacked together, the result is either medium grey (which represents white) or completely black (which represents black).

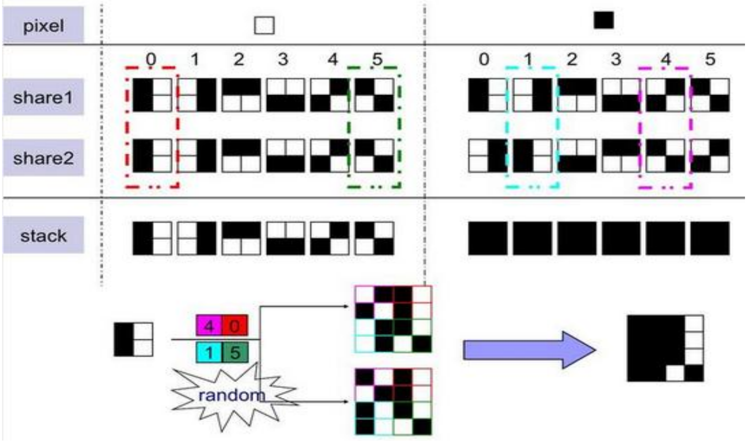


Fig 5 Share creation using VC (2, 2) encryption scheme

Robustness is tested after the watermarked phase of the proposed image share technique. The Watermarked phase is shown below

```
Blocksize = 8     set the size of the block in cover to be used for
each bit in watermark

Determine size of watermark image
Mw = size (watermarked_image, 1)  height
Nw = size (watermarked_image, 2)   width
Define size of original watermark
Mo = height
No = width
x = 1
y = 1
for (kk = 1 : max_message)
dct_block = (watermarked_image (x : x+blocksize-1, y : y+blocksize-1))
if dct_block (5, 2) > dct_block (4, 3)
message_vector (kk) = 0
else
message_vector (kk) = 1
end
move on to next block. At the end of row move to next row.
if (x + blocksize) >= Nw
x = 1
y = y + blocksize
else
x = x + blocksize
end
end
reshape the embedded message
message = reshape (message_vector (1 : Mo * No), Mo, No)
end
```

IV. **RESULT**

1) Peak Signal to Noise Ratio and Mean Square Error: To calculate PSNR, cover image as shown in figure 6 and watermarked image as shown in figure 7, which is a cover image of the image shown in figure 6, are taken and watermarked image is considered as noisy image. Then in a share embedding phase of proposed technique [15] by imposing the mean square error formula and PSNR the simulation result is obtained.

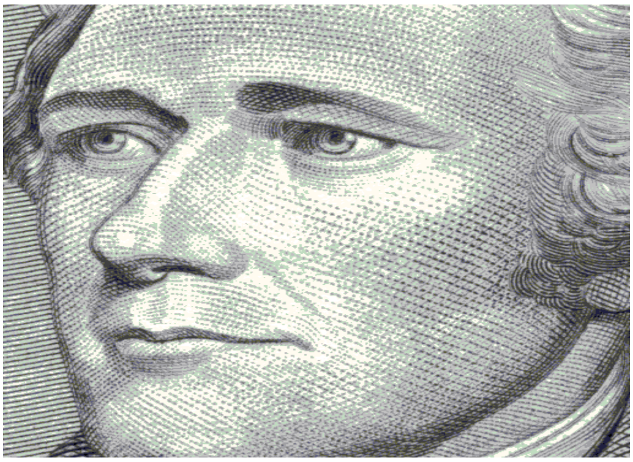


Fig 6 first cover image

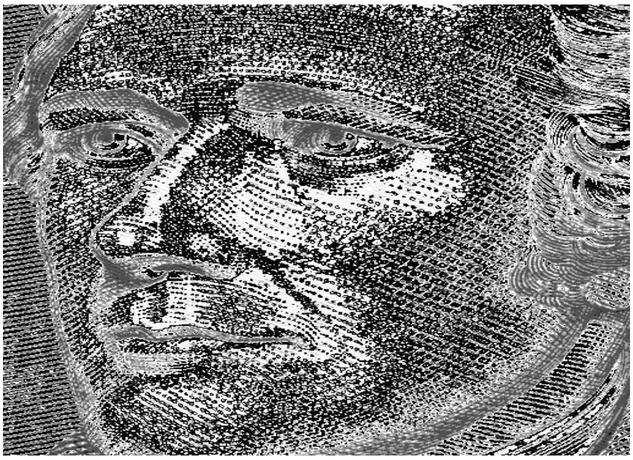


Fig 7 watermarked image 1of first cover image using share 1

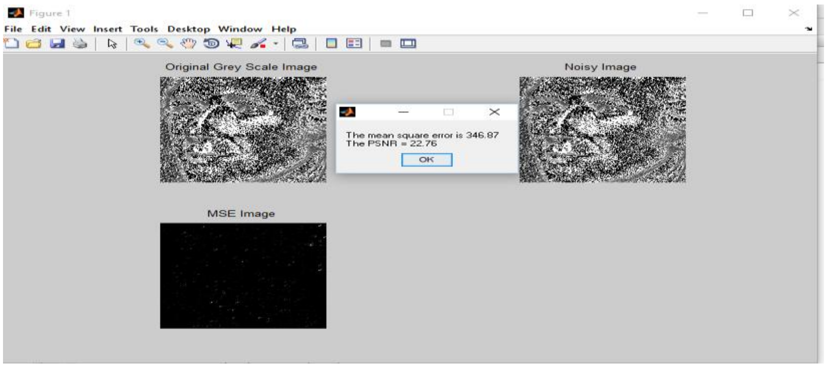


Figure 1
File Edit View Insert Tools Desktop Window Help
Original Grey Scale Image
Noisy Image
MSE Image
OK

The mean square error is 346.87
The PSNR = 22.76

Fig 8 simulation results for PSNR and MSE

"PSNR is used to measure the quality of reconstruction of lossy and lossless compression"[14].The signal in this case is the original cover image, and the blurred image or sharpened image is the error introduced by compression. , PSNR is inversely proportional to the MSE .PSNR is an approximation to human perception of reconstruction quality. Although a higher PSNR generally indicates that the reconstruction is of higher quality, in some cases it may not. Typical standard value for the PSNR in lossy image compression are between 20 and 50 dB .It is must to obtain the PSNR value in this range. In this experiment obtained PSNR value is 22 which significantly identifies the robustness of algorithms against attacks

2) Sharped Images: It is observed that after implementing several attacks to the watermarked image like blurring and sharpening, we are able to reveal the secret image shares. The result is verified by observing the final images generated in the form of message which contains the same meaning of the original message .This result is shown in the figu**r****e**13**.**The end result of this phase contains the original secret images after the attacks.

This result is analysed by observing the extracted messages shown in figure 11 and figure 12 these extracted messages are generated from the digital watermarked images shown in figure 9 and figure 10 respectively .By imposing the purposed technique on the sharped images the messages are revealed back. Figure 13 and Figure 14 shows the revealed message and elapsed time respectively

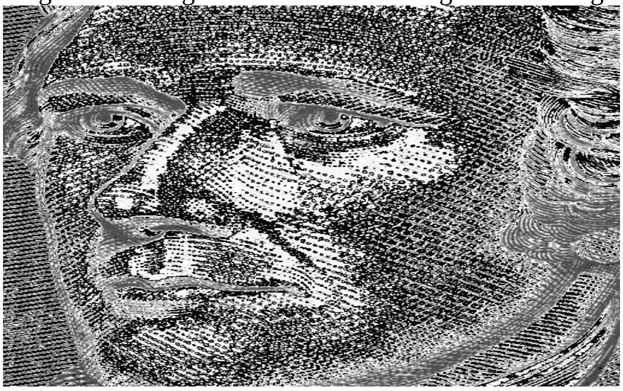


Fig 9 watermarked image 1

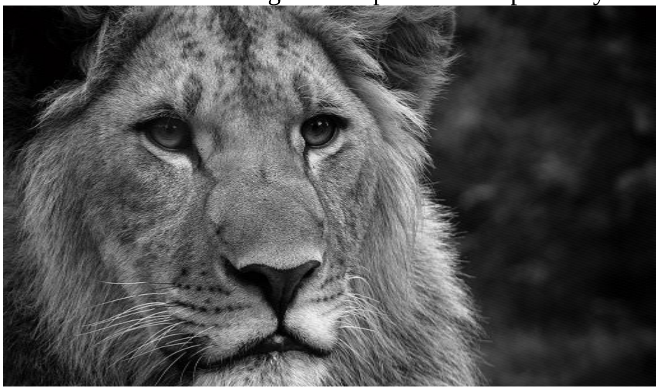


Fig 10 watermarked image 2

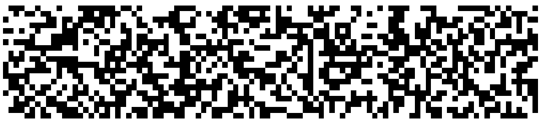


Fig 11 extracted secret message 1

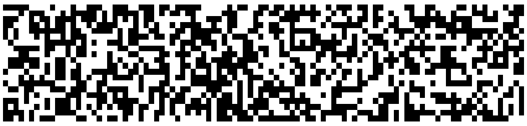


Fig 12 extracted secret message 2

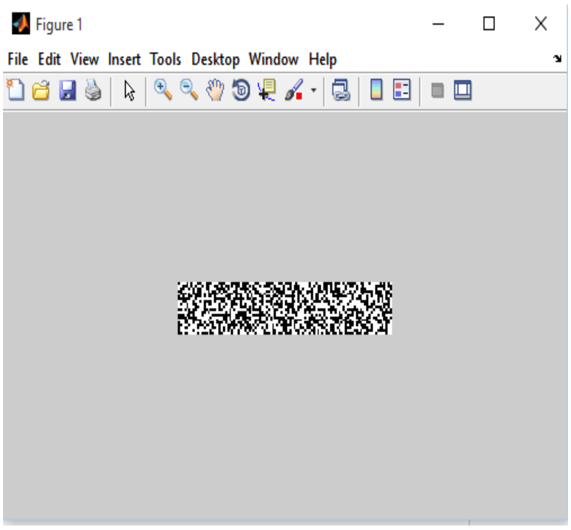
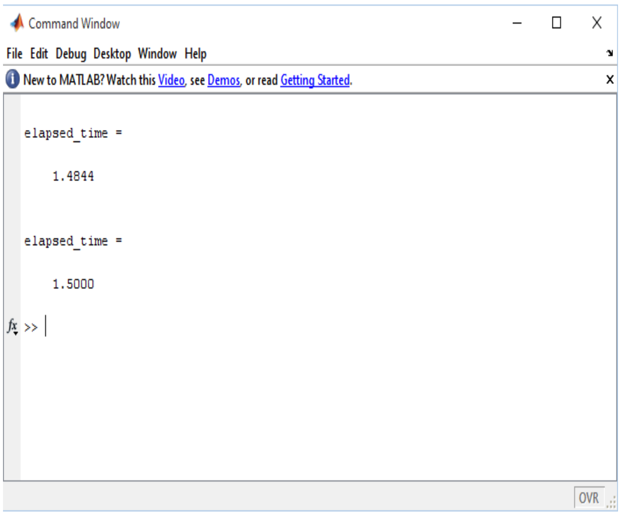


Fig 13 simulation result revealed message for sharp attack


Command Window
File Edit Debug Desktop Window Help
New to MATLAB? Watch this Video, see Demos, or read Getting Started.
OVR

```
elapsed_time =

    1.4844


elapsed_time =

    1.5000

fx >>
```

Fig 14 Elapsed time for image

Elapsed time received from simulation

- Elapsed time of first image is = 1.4844
- Elapsed time of first image is = 1.5000

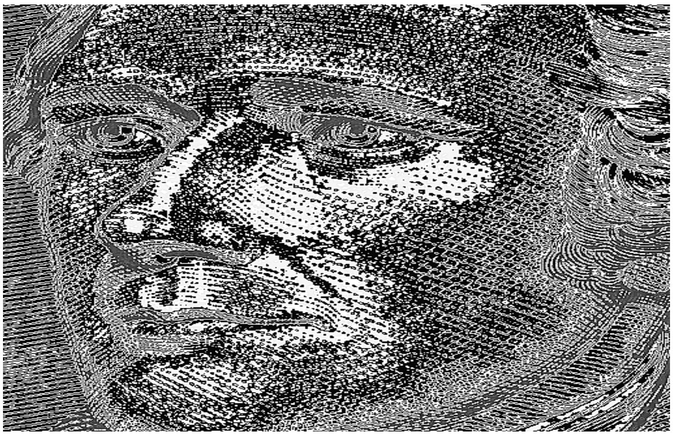


Fig15 Sharp1 images after attack

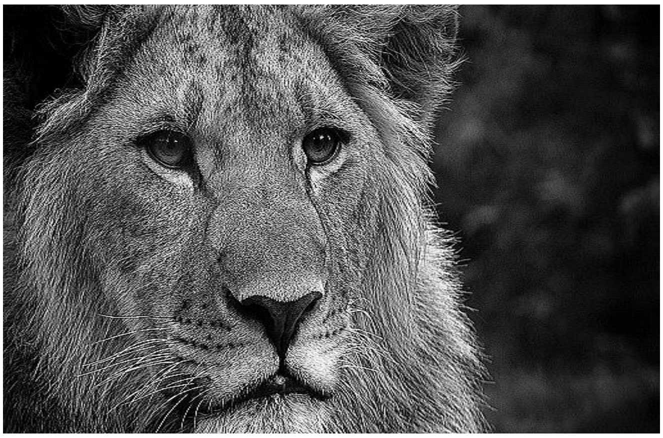


Fig 16sharp2 images after attack

3) *Blurred Images:* To evaluate the robustness of the proposed method, several attacks have been implemented to the watermarked image. Blurring is used in pre-processing steps, such as removal of small details from an image. Noise reduction can be accomplished by blurring with a linear filter and also by nonlinear filtering. After inducing blurring attacks in extracted message as shown in figure19 and figure 20 which are generated from the watermarked images as shown in figure 17 and figure 18 respectively, the simulation results in figure21 shows that the secret images have been extracted successfully from the blurred watermarked images.Figure 22 and Figure 23 are the reveled image messages after the attack.

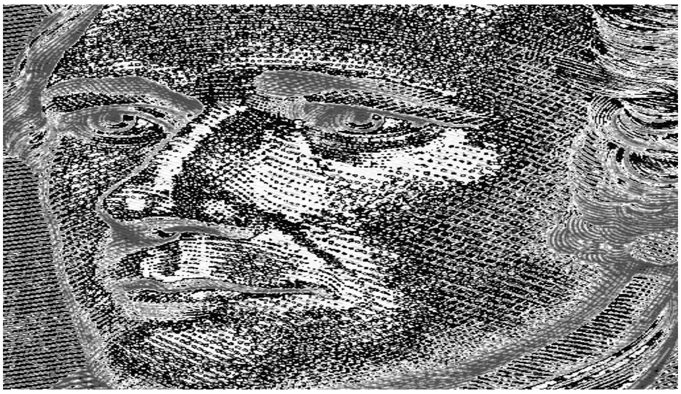


Fig 17 watermarked image 1

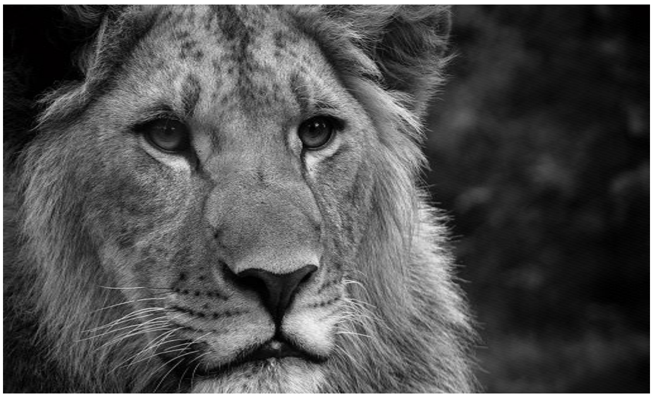


Fig 18 watermarked image 2

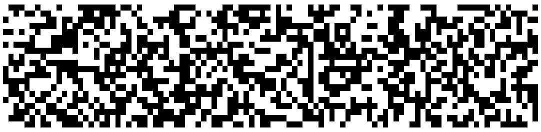


Fig 19 extracted secret message 1

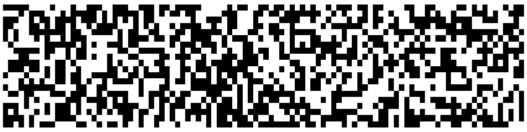


Fig 20 extracted secret message 2

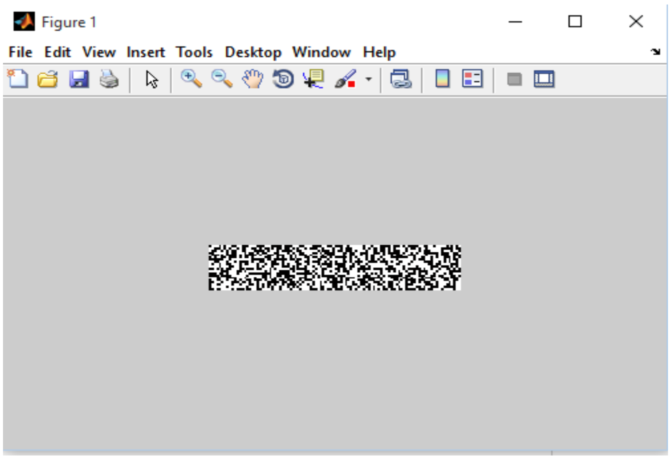
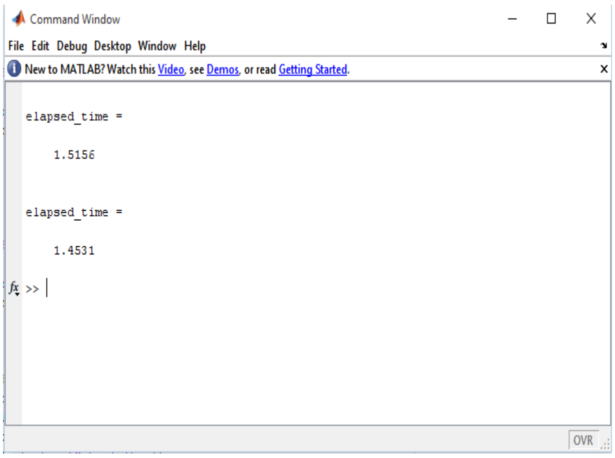


Fig 21 simulation result revealed message for blur attack



New to MATLAB? Watch this Video, see Demos, or read Getting Started.

```
elapsed_time =

    1.5156


elapsed_time =

    1.4531

fx >> 
```

Fig 22 Elapsed time for images

- Elapsed time of first image is = 1.5156
- Elapsed time of first image is = 1.4531

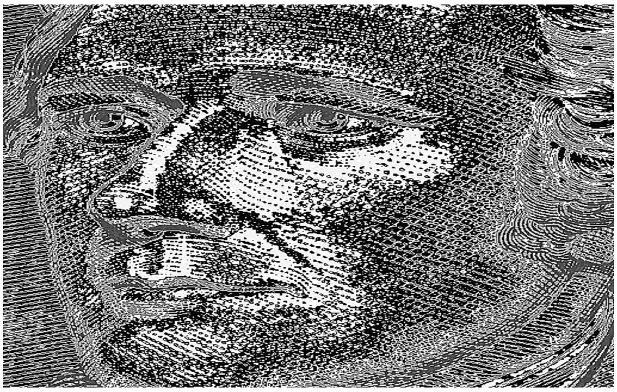


Fig 23 hamilton1 images after attack

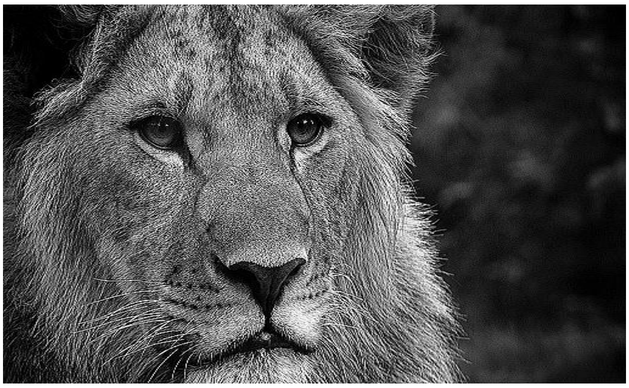


Fig 24 lion image after attack

V. CONCLUSION

The study of the work describes two processes in sequence where first process is an implementation work based on cryptography scheme and the second process is robustness validity check against attacks. This paper concludes the proposed algorithm [15] is well sustainable to the image sharpening and image blurring attacks. The result can be taken into consideration with standard value of PSNR and MSE for the proposed algorithm. The attacks are induced to deform the originality of the message from the image but the proposed algorithm withstands with this attack and provides the quality image at the end that reveals the meaningful message.

REFERENCES

[1] B.padhmavati, P.Nirmal Kumar, M.A.Dorai Rangaswamy, 2010. A Novel Scheme for Mutual Authentication and Cheating Prevention in Visual Cryptography Using Image Processing. In *Proceedings of International Conference on Advances in Computer Science 2010* DOI: 02, ACS.2010.01.264, ACEEE.

[2] E. R. Verheul and H. C. A. Van Tilborg, "Constructions and properties
of out of visual secret sharing schemes," *Designs, Codes, Cryp- tography*, vol. 11, no. 2, pp. 179-196, May 1997.

[3] H. Hajiabolhassan and A. Cheraghi, "Bounds for visual cryptography
schemes," *Discrete Appl. Math.*, vol. 158, no. 6, pp. 659-665, Mar. 2010.

[4] D.Jena and S.Jena, 2009. A Novel Visual Cryptography Scheme. In Proceedings of International Conference on Advanced Computer Control, (ICACC'2009), pp.207-211.

[5] Mrs.D.Mathivadhani, Dr.C.Meena, 2010. Digital Watermarking and Information Hiding using Wavelets, SLSB and Visual Cryptography method. In *Proceedings of International Conference on Computational Intelligence and Computing Research (ICCIC'2010)*, pp. 1-4.

[6] S. J. Shyu, "Image encryption by random grids," *Pattern Recognit.*,
vol. 40, no. 3, pp. 1014-1031, Mar. 2007.

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

[8] P.S.Revenkar, Anisa Anjum, W.Z.Gandhare, 2010. Survey of Visual Cryptographic Schemes. *International Journal of Security and Its Applications*, Vol. 4, No. 2, April, 2010.

[9] S.Punitha, S.Thompson, N.Lingam, 2010. Binary Watermarking Technique based on Visual Cryptography. In *Proceedings of International Conference on Communication Control and Computing Technologies (ICCCCT'2010),* pp. 232-235.

[10] S.Riaz, M.Javed and M.Anjum, 2008. Invisible Watermarking Schemes in Spatial and Frequency Domains. In *Proceedings of fourth International Conference on Emerging Technologies (ICET' 2008)*, pp. 211-216.

[11] Y.Bani, Dr.B.Majhi and R.S.Mangrulkar, 2008. A Novel Approach for Visual Cryptography Using a Watermarking Technique. In *Proceedingsof 2nd National Conference, IndiaCom 2008*.

[12] F. Liu, C. K. Wu, and X. J. Lin, "A new definition of the contrast of
visual cryptography scheme," *Inf. Process. Lett.*, vol. 110, no. 7, pp. 241-246, Mar. 2010.

[13] R. Z. Wang, "Region incrementing visual cryptography," *IEEE Signal
Process. Lett.*, vol. 16, no. 8, pp. 659-662, Aug. 2009.

[14] P. A. Eisen and D. R. Stinson, "Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels," *Designs, Codes, Cryptography*, vol. 25, no. 1, pp. 15-61, 2002.

[15] *Dhirendra Bagri and Dr. R.K.Kapoor "Efficient Approach to find the digital Watermarking ,Cover, Extracted Secret Message using Visual Cryptogrphy",Dhirendra et al ,GJCER,Vol 5(1),2016,113-118*