VISUAL SECRET SHARING

Guided by,

FOUSIA M SHAMSUDEEN

Assistant Professor

Dept.of .MCA

SUBMITTED BY

AYSHAMOL N

NO: 640

INTRODUCTION

- Visual cryptography is a cryptographic technique which allows visual information (pictures,text,) to be encrypted in such a way that the decrypted information appears as a visual image.

- One of the best well known technique was ” VISUAL SECRET SHARING SCHEME”.

- The aim is to maximize the range of the access control of visual secret sharing (VSS) schemes encrypting multiple images

Visual Secret Sharing

- Secret sharing schemes enable a dealer, holding a secret piece of information, to distribute this secret among n participants such a way that only some predefined authorized subsets of participants can resconstruct the secret from their shares and others learn nothing about it
- It’s a method of dividing a secret image among a group pf participants
- Example : k by n scheme (k,n) { if k=n then all participants are required to reconstruct the secret }

OBJECTIVES

The main objectives are :-

- Secure information storage.
- Computational speed and transmission rate can be made so faster by the help of DCT.
- A good security is provided by the use of encryption and decryption techniques.
- Embed maximum amount of additional data without causing any distortion to the cover media..

REVIEW OF LITERATURE

- ✓ S. J. Shyu and K. Chen, “Visual multiple-secret sharing by circle random grids,” SIAM J. Imag. Sci., vol. 3, no. 4, pp. 926–953, 2010.

- ✓ M. Sasaki and Y. Watanabe, “Formulation of visual secret sharing schemes encrypting multiple images,” in Proc. 39th IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP), Jun. 2014, pp. 7391–7395.
- ✓ M. Bose and R. Mukerjee, “Optimal (k,n) visual cryptographic schemes for general k,” Des., Codes Cryptogr., vol. 55, no. 1, pp. 19–35, 2010. [7]
- ✓ Y.-C. Chen, “Fully incrementing visual cryptography from a succinct non-monotonic structure,” IEEE Trans. Inf. Forensics Security, vol. 12, no. 5, pp. 1082–1091, May 2017.

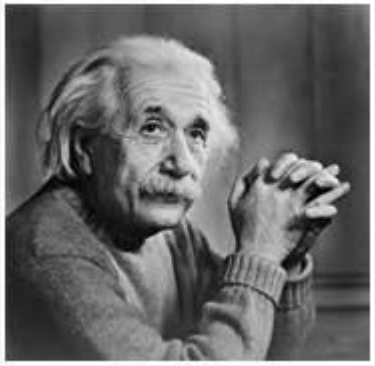
- ✓ R. Z. Wang, “Region incrementing visual cryptography,” IEEE Signal Process. Lett., vol. 16, no. 8, pp. 659–662, Aug. 2009. [25]
- ✓ S. Washio and Y. Watanabe, “Security of audio secret sharing scheme encrypting audio secrets with bounded shares,” in Proc. 39th IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP), May 2014, pp. 7396–7400. [26]
- ✓ C.-N. Yang and T.-H. Chung, “A general multi-secret visual cryptography scheme,” Opt. Commun., vol. 283, no. 24, pp. 4949–4962, 2010.
- ✓ R. Gonzalez and R. Woods, “Digital Image Processing,” Prentice Hall, Englewood Cliffs, NJ, 2002
- ✓ https://www.mathworks.com/help/images/discrete-cosine-transform.html#bq59tsh

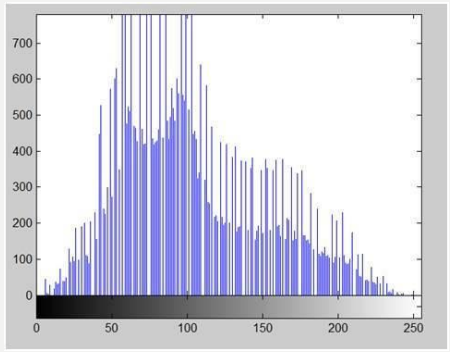
METHODOLOGY

1) Image histogram processing

Histogram is a graph , A graph that shows frequency of anything usually it shows frequency of occuring of datas in the whole dataset. But an image histogram, shows frequency of pixels intensity values. In an image histogram, the x axis shows the gray level intensities and the y axis shows the frequency of these intensities.

Example :





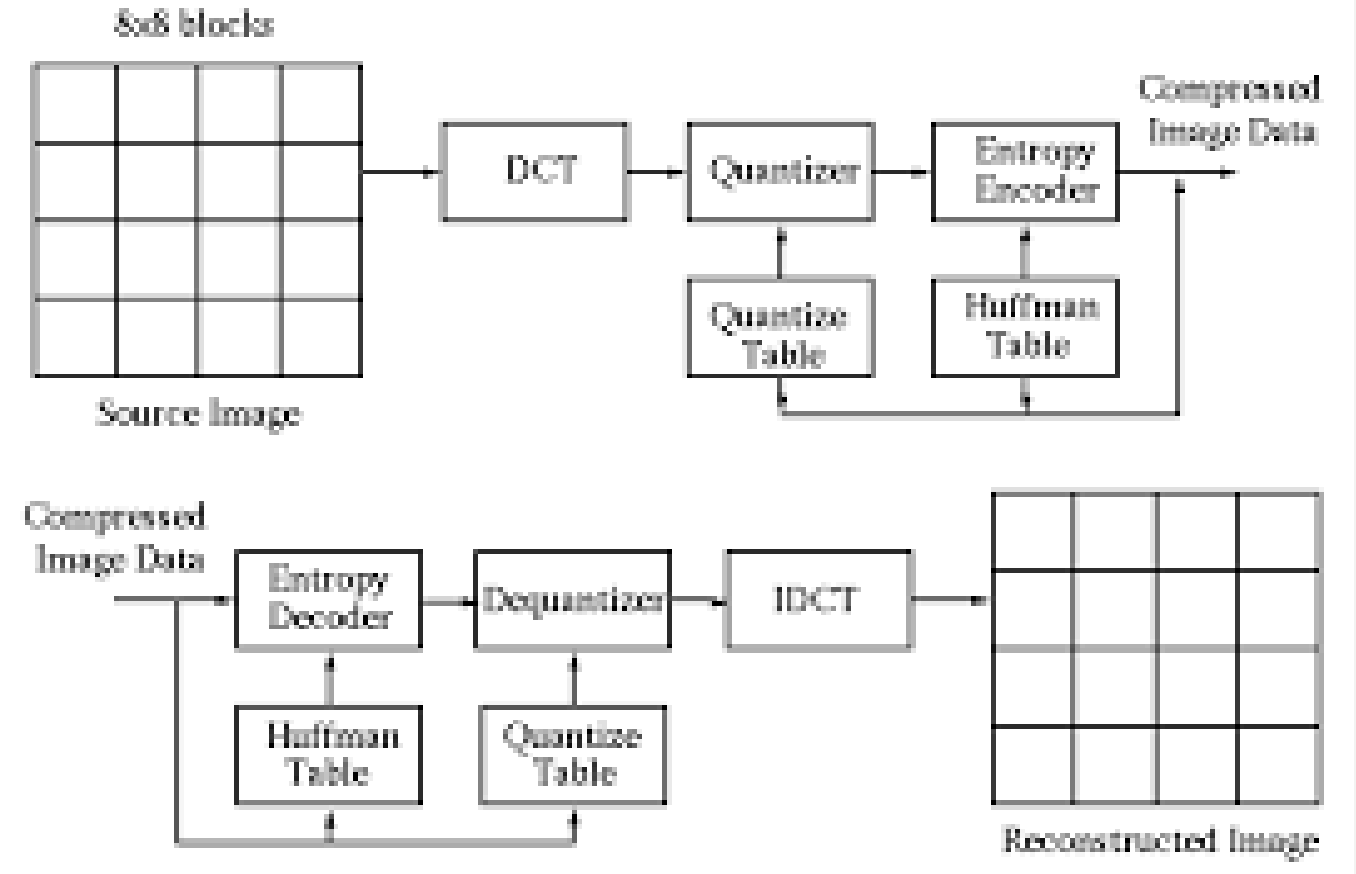
CONT…

2. Discrete cosine transform ::

- DCT is an example of transform method.it simply trying to compress the pixel values directly,the image is first transformed into the frequency domain and it will eliminate the high frequency values.
- low frequency coefficients usually have more energy than high frequency
- The human visual system is more sensitive to low frequencies

CONT…

❖**Working of DCT…**



CONT…

3. Share Division

- In the proposed system (k,n) 2<=k<=n ,secret sharing scheme,n noise like shares are generated from a secret image .
- First of all secret image matrix is found out then the system will randomly generate a matrix called ri.
- Then the secret image is XOR-
- with the randomized matrix ri and the resultant will be the first share.
- Now the input of first share will be XOR-ed with randomised matrix ri to produce the second share.

CONT…

3. LSB EMBEDDING

- Least Significant Bit (LSB) embedding is a simple strategy to implement steganography
- It embeds the data into the cover so that it cannot be detected by a casual observer.
- The technique works by replacing some of the information in a given pixel with information from the data in the image

CONT…

4. Encryption and decryption

- RC4 was designed by Ron Rivest of RSA Security in 1987.
- It is a symmetric key algorithm which included in stream cipher
- A stream cipher generates what is called a key stream(a sequence of bits used as a key)
- Encryption is accomplished by combining the key stream with the plaintext , usually with the bitwise XOR operation

PROPOSED SYSTEM...

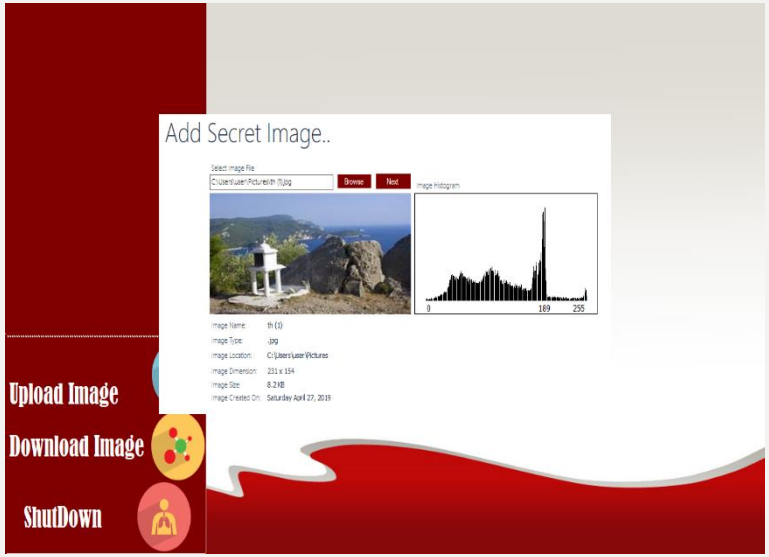
STAGES

STEP 1: UPLOAD THE IMAGE
STEP2 : IMAGE HISTOGRAM
STEP3 : APPLYING DCT
STEP4 : SHARE DIVISION
STEP5 : EMBED SHARES
(SELECT CARRIER IMAGES)
STEP6 : ENCRYPTION
STEP7 : SAVING IMAGES
STEP8 : LOAD CARRIER IMAGES
(EXTRACT SHARES)
STEP9 : DECRYPTION
STEP10: RECONSTRUCT SECRET IMAGE
STEP11: INVERSE DCT
STEP12: EXTRACT SECRET IMAGE

SCREENSHOTS……

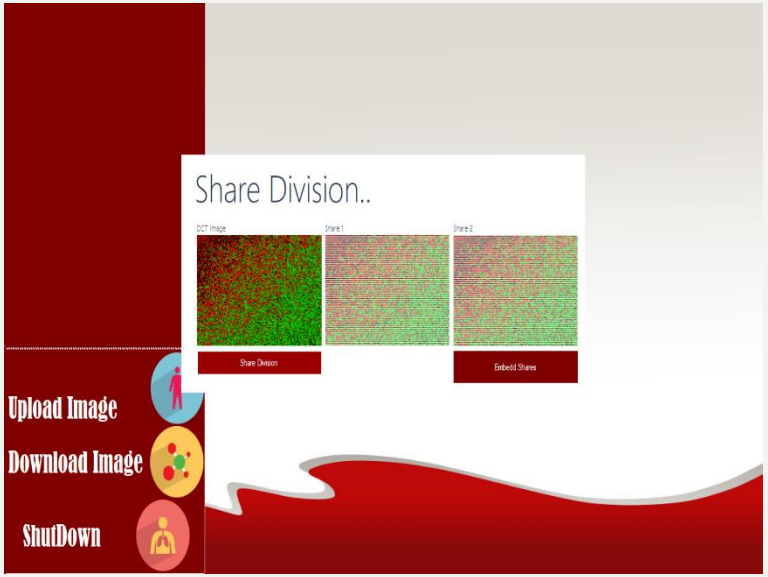
❖LOGIN PAGE

❖IMAGE UPLOADING

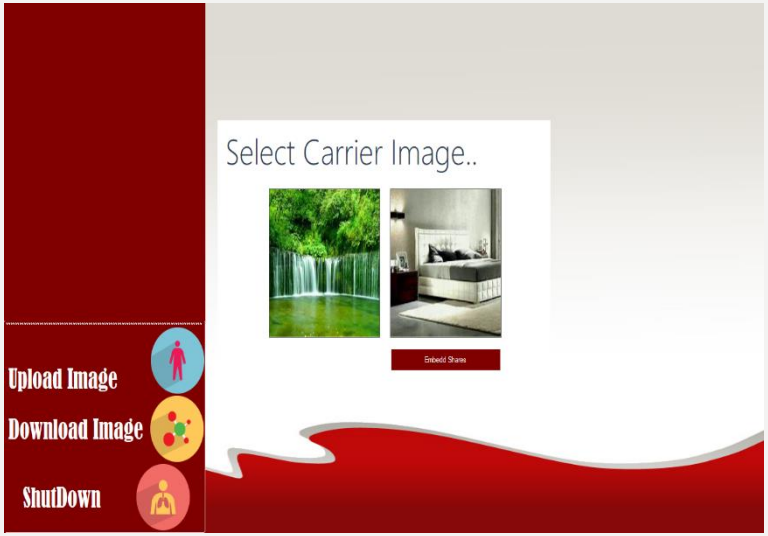


❖ DCT…

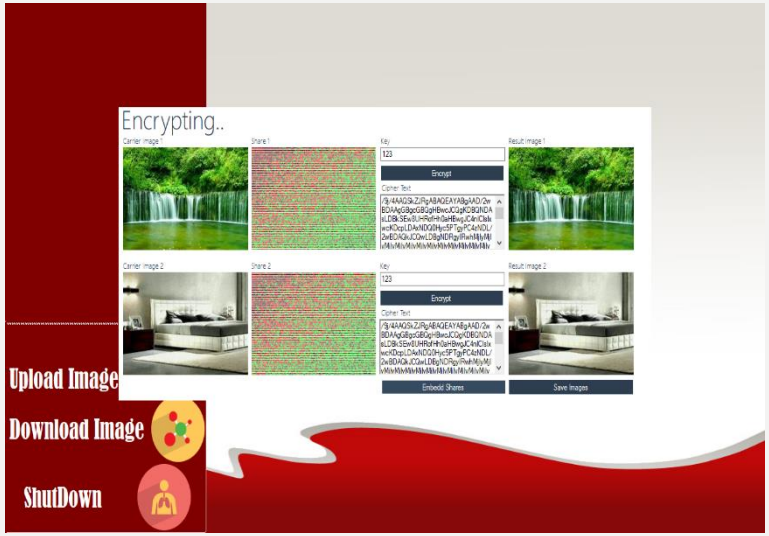
❖ SHARE DIVISION…



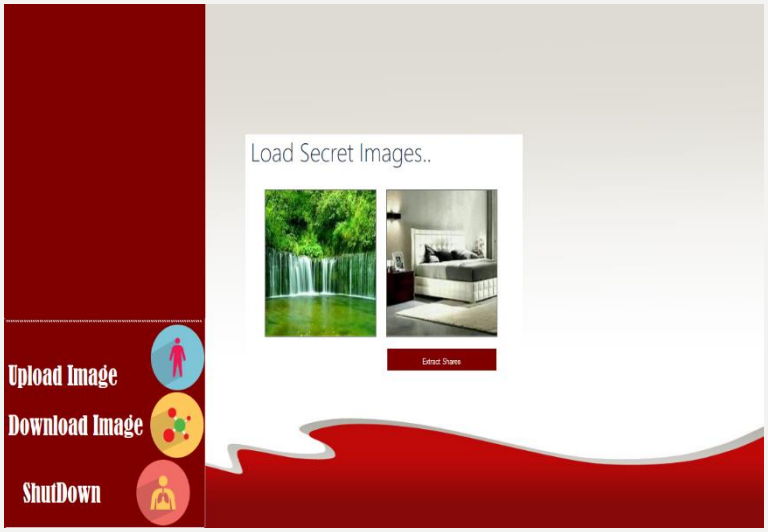
❖ CARRIER IMAGES



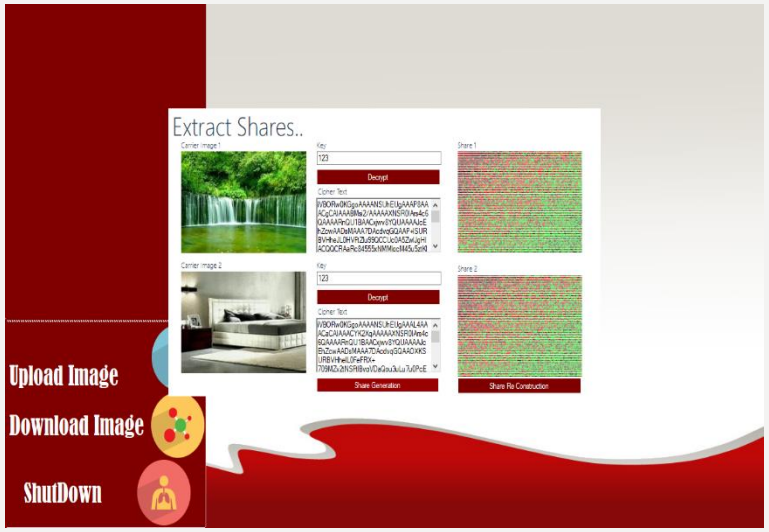
❖ ENCRYPTION



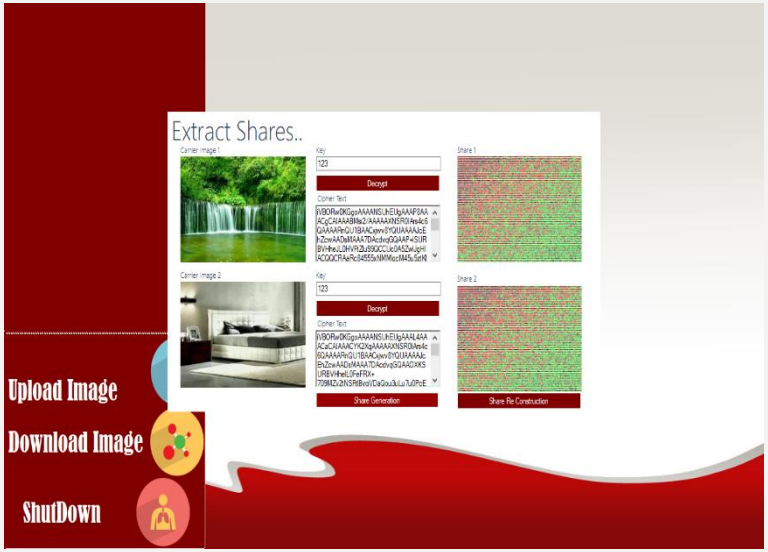
❖ LOAD IMAGES



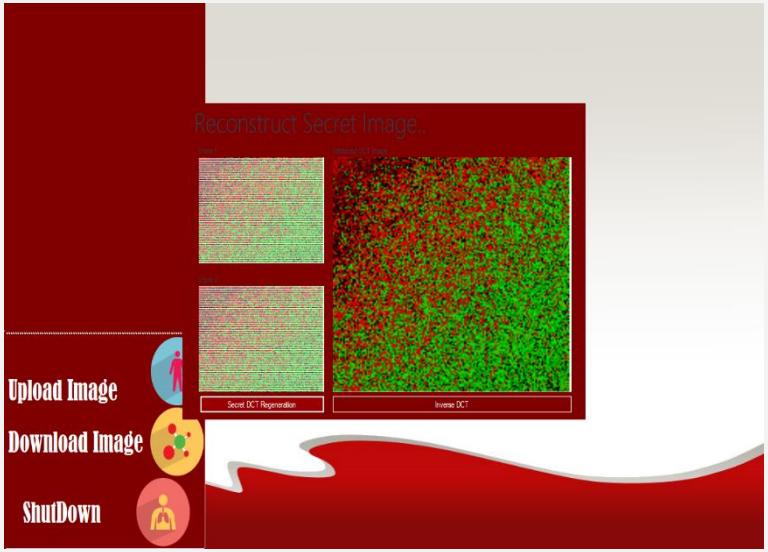
❖ DECRYPTION



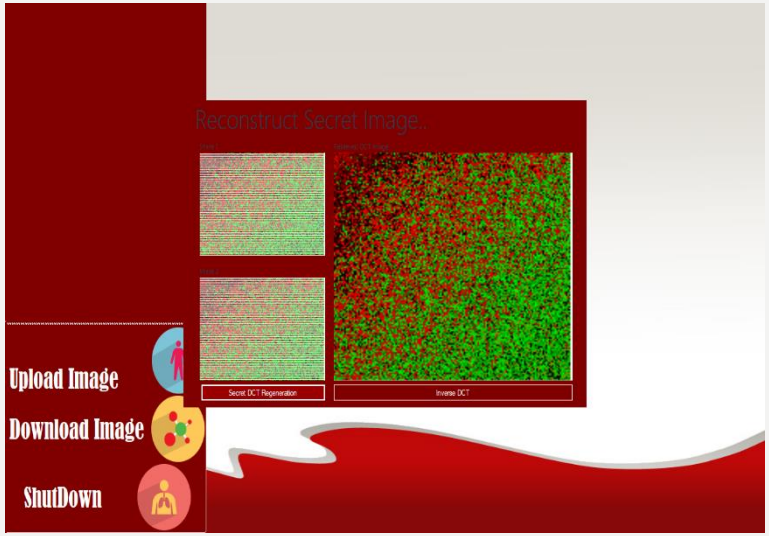
❖ SHARES…



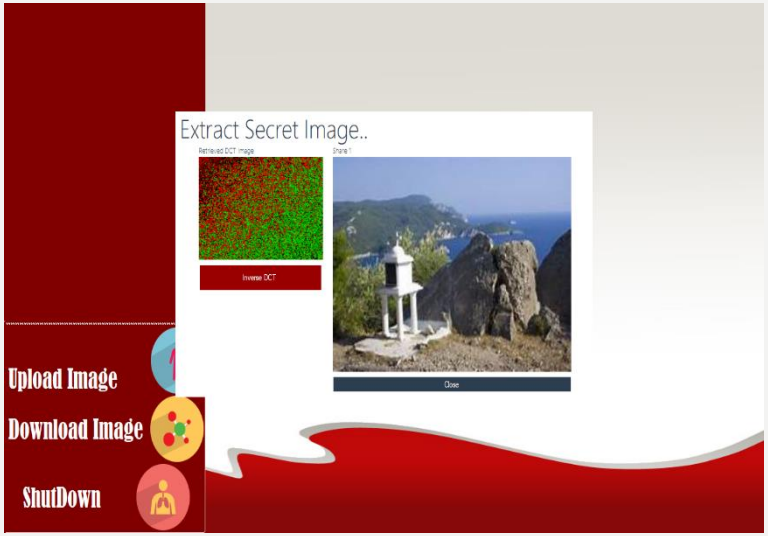
❖ RECONSTRUCTION



❖ INVERSE DCT



❖ SECRET IMAGE



CONCLUSION

- The proposed scheme is able to encrypt images and decrypt them successfully without degrading the quality of the images.
- In terms of contrast ,computational speed and transmission rate, this system is observed to be superior than normal vss schemes.
- The proposed scheme is able to encrypt multiple number of images and decrypt them successfully without degrading the quality of the images.

REFERENCES

- [1] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, “Extended capabilities for visual cryptography,”
- M. Naor and A. Shamir, “Visual cryptography,” in Proc. EUROCRYPT
- Multiple Image Sharing Scheme using Visual Cryptography 1Dr. Ch. Samson, 2Masabattula N S Durgamba 1Associate Head, Dept. of Information Technology, SNIST, Hyderabad, Telangana, India (paper published in www.ijarcsse.com)
- M. Iwamoto and H. Yamamoto, “A construction method of visual secret sharing schemes for plural secret images,” IEICE Trans. Fundam., vol. 86, no. 10, pp. 2577–2588, 2003.
- M. Naor and B. Pinkas, “Visual authentication and identification,” in Advances in Cryptology—CRYPTO (Lecture Notes in Computer Science), vol. 1294. Berlin, Germany: Springer-Verlag, 1997, pp. 322–336.
- M. Naor and A. Shamir, “Visual cryptography,” in Advances in Cryptology—EUROCRYPT (Lecture Notes in Computer Science), vol. 950. Berlin, Germany: Springer-Verlag, 1994, pp. 1–12.
- M. Sasaki and Y. Watanabe, “Formulation of visual secret sharing schemes encrypting multiple images,” in Proc. 39th IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP), Jun. 2014, pp. 7391–7395. [.

THANK YOU!