A Secure Image based Steganography and Cryptography with Watermarking

Sarita Poonia, Mamtesh Nokhwal, Ajay Shankar

Abstract*— *In this paper we uses the steganography and cryptography techniques with the watermarking so that to protect the particular information. Steganography is accomplished through hiding the information in the other information, thus by hiding the existence of the communicated information and steganography can be amplified by combining it with the cryptography and watermarking. And the cryptography is used for the security purpose. Cryptography uses two main styles or forms of encrypting data, symmetrical and asymmetrical. Watermarking technology is used for copyright protection of images, audios and videos. Watermarking process to signal modulation model. The basic idea of the proposed system is that it will allow an average user to securely transfer the text information by hiding them in a digital image file using the local characteristics within the image, which will provide a strong backbone for its security.

Keywords*- *Cryptography, PSNR, steganography, Water marking.

I. INTRODUCTION

In this paper we proposed a system in which the image is being secured by steganography and cryptography with watermarking so as to protect the data more easily. A combination of stegnography and cryptography algorithms with watermarking, which provides a strong backbone for its security. The proposed system not only hides large volume of data within an image, but also limits the perceivable distortion that might occur in an image while processing it. This paper has an advantage over other information security systems because the hidden text is in the form of images, which are not obvious text information carriers.

A. Steganography.

Steganography is an art of transferring message in a way that the existence of message is concealed. Steganography can utilize various medium as carriers of the message. These mediums may include the classical methods of steganography using text, like character marking, invisible ink, using pin pictures, type-writer correction), images, and audio, video signals. The most common approaches to information hiding in images are: Least significant bit (LSB) insertion, Masking and filtering techniques, Algorithms and transformations. Masking and filtering techniques hide information by marking an image in a manner similar to paper watermarks. Because watermarking techniques are more integrated into the image, they may be applied without fear of image destruction from lossy compression.

The least significant bit insertion (LSB) is the most widely used image steganography technique. It embeds message in the least-significant bits of each pixel. The LSB techniques might use a fixed least significant bit insertion scheme, in which the bits of data added in each pixel remains constant, or a variable least significant bit insertion, in which the number of bits added in each pixel vary on the surrounding pixels, to avoid degrading the image fidelity In this paper we discuss the embedding of text into image through variable size least significant bit insertion. Today, computer and network technologies provide easy-to-use communication channels for steganography. Essentially, the information-hiding process in a steganographic system starts by identifying a cover medium's redundant bits.

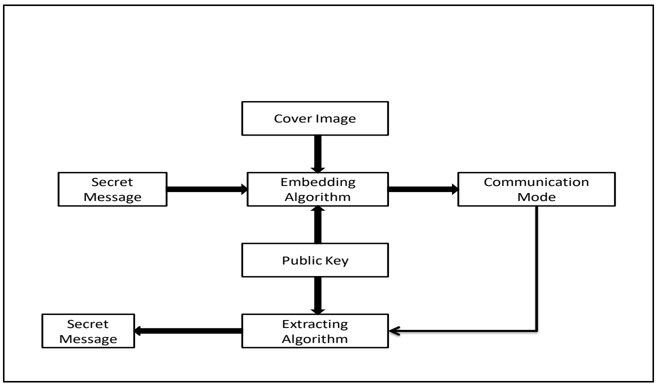


Figure1: Basic Layout of Image Steganographic System

B. Cryptography.

In today's information age, information sharing and transfer has increased exponentially. Cryptography can be defined as the conversion of data into a scrambled code that can be deciphered and sent across a public or private network. Cryptography uses two main styles or forms of encrypting data; symmetrical and asymmetrical. Symmetric encryptions, or algorithms, use the same key for encryption as they do for decryption. Other names for this type of encryption are secret-key, shared-key, and private-key. Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. A cryptographic algorithm, or cipher, is a mathematical function used in the encryption and decryption process. A cryptographic algorithm works in combination with a key—a word, number, or phrase—to encrypt the plaintext.

Manuscript received on June, 2013.

Mamtesh Nokhwal, Guru Jambheshwar University of Science & Technology, Hisar, India.
Sarita Rani, Guru Jambheshwar University of Science & Technology, Hisar, India.
Dr. Ajay Shankar, Guru Jambheshwar University of Science & Technology, Hisar, India.

The same plaintext encrypts to different ciphertext with different keys. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key. A cryptographic algorithm, plus all possible keys and all the protocols that make it work comprise a cryptosystem. We use encryption to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting ciphertext to its original plaintext is called decryption. Figure 1-1 illustrates this process.

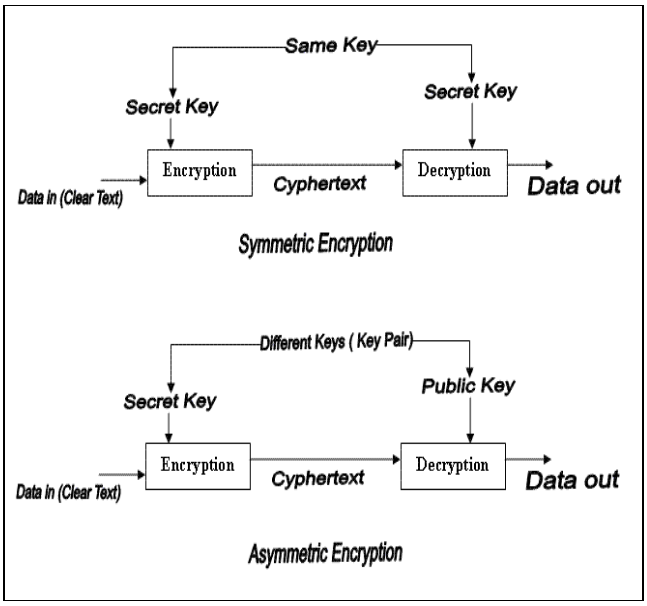


Figure 2 : Basic types of encryption.

C. Digital Watermarking

A digital watermark is a piece of information which is embedded in the digital media and hidden in the digital content in such a way that it is inseparable from its data. This piece of information known as watermark, a tag, or label into multimedia object such that the watermark can be detected or extracted later to make an assertion about the object. The object may be an image, audio, video, or text. This paper is focused on noteworthy work and techniques used for images during preliminary and principal development stage of digital watermarking by various researchers with the utility of giving a fundamental understanding of the basic principles of digital watermarking as it has evolved. This may serve as the concrete foundation and the base for understanding further advances in this technology in later years. This paper gives a summary of different innovative techniques in this emerging area.

Watermarking is the process of inserting a digital signal or pattern (indicative of the owner of the content) into digital content. The signal, known as a watermark, can be used later to identify the owner of the work, to authenticate the content, and to trace illegal copies of the work.

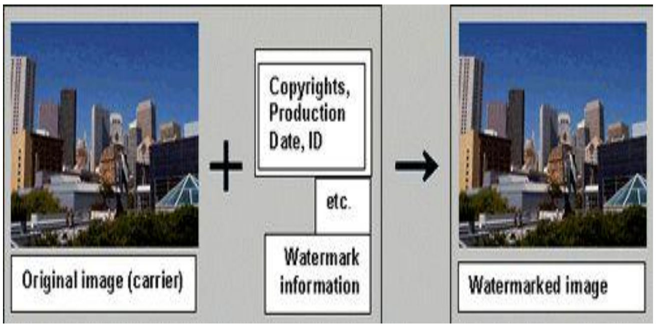


Figure 3: The Basic Structure of Digital Watermark.

II. PROPOSED SYSTEM

In the steganographic system we basically used the Least Significant Bit technique.

The general usage of information hiding and watermarking or else provide an overview of detection algorithms. Here, we present recent research and discuss the practical application of detection algorithms and the mechanisms for getting around them.

Apply of LSB technique during discrete cosine transformation (DCT) on cover image.

The following steps are followed in this case: -

1. The Image is broken into data units each of them consists of 8 x 8 block of pixels.
2. Working from top-left to bottom-right of the cover image, DCT is applied to each pixel of each data unit.
3. After applying DCT, one DCT Coefficient is generated for each pixel in data unit.
4. Each DCT coefficient is then quantized against a reference quantization table.
5. The LSB of binary equivalent the quantized DCT coefficient can be replaced by a bit from secret message.
6. Encoding is then applied to each modified quantized DCT coefficient to produce compressed Stego Image.

When the embedded data’s bits are substituted into the least significant bits (LSB’s) location it will have little to no effect on the images appearance to the human eye. The software used to embed the hidden file will usually zero out the LSB’s. Once these bits are zeroed out they are ready to be used by the steganography software to contain whatever data is going to be embedded. Digital watermarking, also known as “fingerprinting” is in its infancy stage of development. Many different companies are developing different types of watermarking but they all basically work in the same manner. Most of the technology is being developed for use as a copyright protection and licensing tool. Digital watermarking can be used on any digital image, audio file or text file. Much like the watermarking of old, digital watermarking is used to signify ownership and source authenticity.

In conventional cryptography, also called secret-key or symmetric-key encryption, one key is used both for encryption and decryption.

Pretty Good Privacy (PGP) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting and decrypting texts, e-mails, files, directories and whole disk partitions to increase the security of e-mail communications.

PGP combines some of the best features of both conventional and public key cryptography. PGP is a hybrid cryptosystem. When a user encrypts plaintext with PGP, PGP first compresses the plaintext. PGP then creates a session key, which is a one-time-only secret key. This key is a random number generated from the random movements of your mouse and the keystrokes you type. This session key works with a very secure, fast conventional encryption algorithm to encrypt the plaintext; the result is ciphertext. Once the data is encrypted, the session key is then encrypted to the recipient's public key. This public key-encrypted session key is transmitted along with the ciphertext to the recipient. Decryption works in the reverse. The recipient's copy of PGP uses his or her private key to recover the temporary session key, which PGP then uses to decrypt the conventionally-encrypted ciphertext.

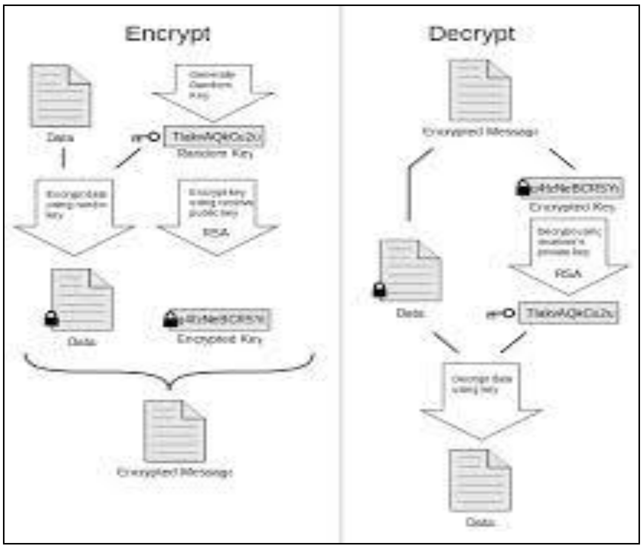


Figure 4: PGP Encryption and Decryption

Watermarks are a way of dealing with the problems mentioned above by providing a number of services:

1. They aim to mark digital data permanently and unalterably, so that the source as well as the intended recipient of the digital work is known. Copyright owners can incorporate identifying information into their work. That is, watermarks are used in the protection of ownership. The presence of a watermark in a work suspected of having been copied can prove that it has been copied.

2. By indicating the owner of the work, they demonstrate the quality and assure the authenticity of the work.

3. With a tracking service, owners are able to find illegal copies of their work on the Internet. In addition, because each purchaser of the data has a unique watermark embedded in his/her copy, any unauthorized copies that s/he has distributed can be traced back to him/her.

4. Watermarks can be used to identify any changes that have been made to the watermarked data.

5. Some more recent techniques are able to correct the alteration as well.

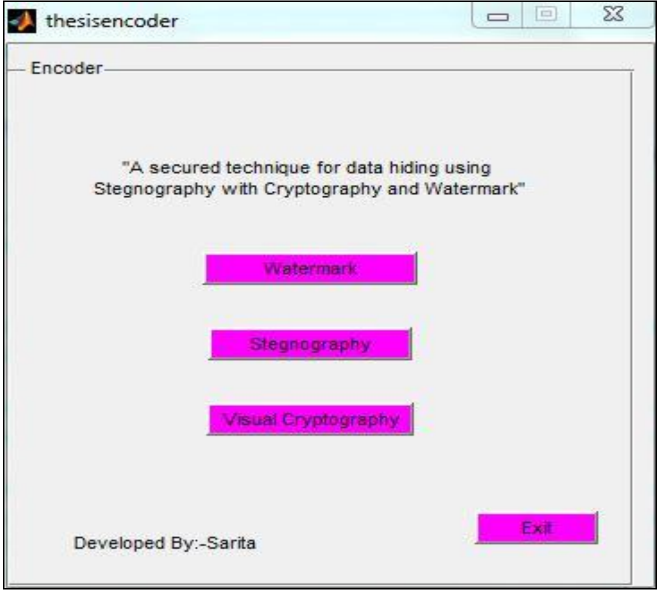
Watermarks can be visible or invisible:

1. *Visible* watermarks are designed to be easily perceived by a viewer (or listener). They clearly identify the owner of the digital data, but should not detract from the content of the data.

2. *Invisible* watermarks are designed to be imperceptible under normal viewing (or listening) conditions; more of the current research focuses on this type of watermark than the visible type.

In this proposed system we uses the invisible watermarks. In the Invisible Watermarks we uses the license Key so as to protect the information and this can be carried out with the help of the cryptography, in which we use the public or private key. And after we get the shares. These are shown in the following figures.

These are also divided into encoder and decoder part. The encoder is part is used to encrypt the data into the image whereas the decoder part decrypt the data from the encrypted image.

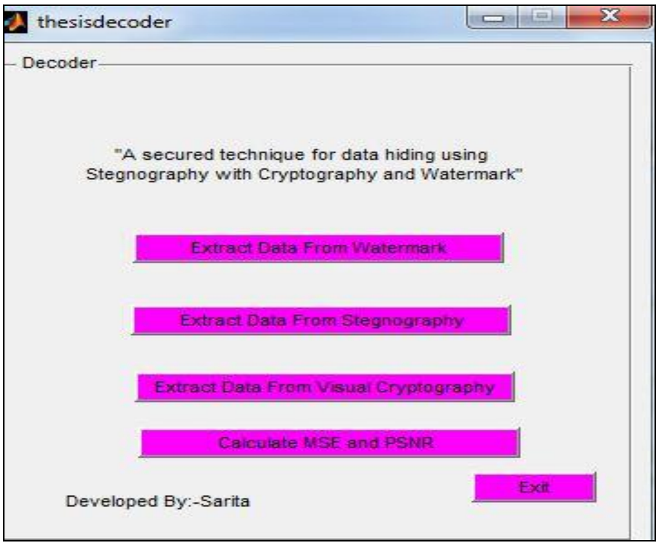

thesisencoder

Encoder

"A secured technique for data hiding using Stegnography with Cryptography and Watermark"

Developed By:-Sarita

Figure 5: The encoder part of the proposed system


thesisdecoder

Decoder

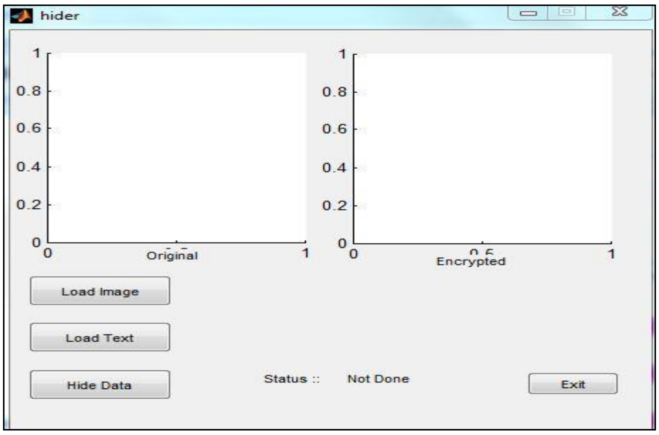
"A secured technique for data hiding using Stegnography with Cryptography and Watermark"

Developed By:-Sarita
Extract Data From Watermark
Extract Data From Stegnography
Extract Data From Visual Cryptography
Calculate MSE and PSNR
Exit

Figure 6: The Decoder part of the proposed system

The GUI which is created for the steganography part is that in which we load the original image and in which we insert the information, these all are done with the LSB technique.

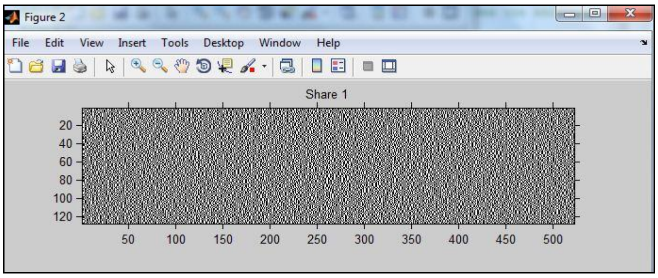
Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication



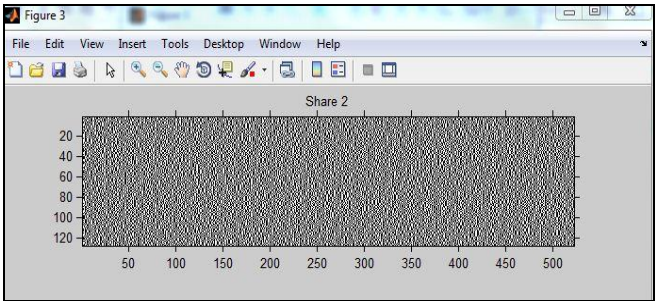
Status :: Not Done

Figure 7: The GUI created for the Steganography.

The visual cryptography will divide the image into the shares, which on overlapping will provide the required output, the information.



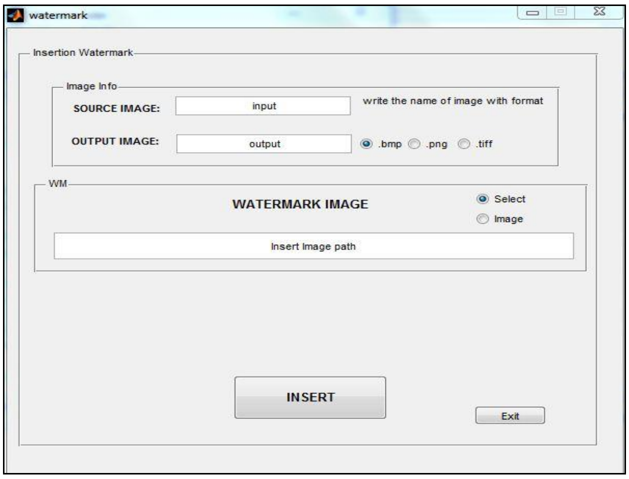
Share 1



Share 2

Figure 8: It consists of the Share1 and Share 2.

These are various GUI created for the function performed for the watermark, steganography and cryptography. All these functions can be performed in a single system.



SOURCE IMAGE: input

OUTPUT IMAGE: output ● .bmp ○ .png ○ .tiff

● Select ○ Image

Insert Image path

Figure 9: The GUI is created for the watermark operation

There are a few different ways to ensure that a file is not readily accessible to everyone. The most common methods would be encryption, steganography and watermarking. Though these are all somewhat similar technologies they are a world apart in how they do their job. When a file is encrypted it takes the information and puts it into a format that hopefully only the people who have the right keys can open the document. When the document is sent across the Internet anyone who can capture the document can see that it has been encrypted and there is that possibility that the document could be decrypted. By using steganography the file is completely hidden from anyone's eyes. This way of sending hidden documents or images is truly hidden. At the present time there are literally hundreds of freeware and shareware programs on the Internet. Discovery and destroying covert information within steganographic files is called steganalysis. As steganalysis becomes more mature it will be implemented as a standard security tool the way firewalls, virus detection software and intrusion detection programs currently are. Steganalysis is used to discover and remove hidden files. Many times the same programs or algorithm used to hide a file for legitimate reasons, such as a watermark, would be the same one that is used to hide a file that a user didn't want discovered. Repetitive or obvious signs of manipulation are the easiest way to try and detect hidden files or messages, but this is usually not possible with the human eye. Images that are hidden using Image domain type of software are easier to destroy then the Transform domain type. One easy way to destroy Image domain type images is to convert their compression type from lossless to lossy. By converting a Bitmap or Gif file to a JPEG file will many times destroy the hidden file within because of the different types of compression. Each type of steganography software has its own unique signature that is left on a file. Once this signature is known a mathematical expression can be developed and then that expression is used to compare one file with another to see what deviations occurred.

We also calculate the Peak Signal to Reconstructed Image.

Signal-to-noise (SNR) measures are estimates of the quality of a reconstructed image compared with an original image. The basic idea is to compute a single number that reflects the quality of the reconstructed image.

The actual metric we will compute is the peak signal-to-reconstructed image measure which is called PSNR. Assume we are given a source image f(i,j) that contains N by N pixels and a reconstructed image F(i,j) where F is reconstructed by decoding the encoded version of f(i,j). Error metrics are computed on the luminance signal only so the pixel values f(i,j) range between black (0) and white (255).

First you compute the mean squared error (MSE) of the reconstructed image as follows

$$\mathrm{MSE} = \frac{\sum[f(i,j) - F(i,j)]^2}{N^2}$$

The summation is over all pixels. The root mean squared error (RMSE) is the square root of MSE. Some formulations use N rather N^2 in the denominator for MSE.

PSNR in decibels (dB) is computed by using

$$\mathrm{PSNR} = 20\log_{10}\left(\frac{255}{\mathrm{RMSE}}\right)$$

In the previous equation, R is the maximum fluctuation in the input image data type. For example, if the input image has a double-precision floating-point data type, then R is 1. If it has an 8-bit unsigned integer data type, R is 255, etc.

III. CONCLUSION

In this paper we have presented a new system for the combination of cryptography and Steganography with Watermarking which could be proven as a highly secured method for data communication in near future. Steganography, especially combined with cryptography and watermarking is a powerful tool which enables people to communicate without possible eavesdroppers even knowing there is a form of communication in the first place. The proposed method provides acceptable image quality with very little distortion in the image. The main advantage of this System is to provide high security for key information exchanging. It is also useful in communications for codes self error correction. It can embed corrective audio or image data in case corruption occurs due to poor connection or transmission. The proposed High secured system using cryptography, steganography and watermarking is tested by taking message and hiding them in some images of different sizes. The results that are obtained from these experiments are recorded.

REFERENCES

1. N . Provos, “Defending Against Statistical Steganography,” Proc 10th USENEX Security Symposium 2005.
2. N . Provos and P. Honeyman, “Hide and Seek: An introduction to Steganography,” IEEE Security & Privacy Journal 2003.
3. Steven W. Smith , The Scientist and Engineer's Guide to Digital Signal Processing.
4. Katzenbeisser and Petitcolas , ”Information Hiding Techniques for Stenography and Digital watermaking” Artech House, Norwood, MA. 2000.
5. L. Reyzen And S. Russell , “More efficient provably secure Steganography” 2007.
6. S.Lyu and H. Farid , “Steganography using higher order image statistics , “ IEEE Trans. Inf. Forens. Secur. 2006.
7. Venkatraman , s, Abraham , A . & Paprzycki M.” Significance of Steganography on Data Security “ ,Proceedings of the International Conference on Information Technology : coding and computing , 2004.
8. Fridrich , J ., Goljan M., and Hogea , D ; New Methodology for Breaking stenographic Techniques for JPEGs. “Electronic Imaging 2003”.
9. http:/ aakash.ece.ucsb.edu./data hiding/stegdemo.aspx.Ucsb data hiding online demonstration. Released on Mar .09,2005.
10. Mitsugu Iwanmoto and Hirosuke Yamamoto, “The Optimal n-out-of-n Visual Secret Sharing Scheme for GrayScale Images”, IEICE Trans. Fundamentals, vol.E85- A, No.10, October 2002, pp. 2238-2247.
11. Doron Shaked, Nur Arad, Andrew Fitzhugh, Irwin Sobel, “Color Diffusion: Error Diffusion for Color Halftones”, HP Laboratories Israel, May 1999.
12. Z.Zhou, G.R.Arce, and G.Di Crescenzo, “Halftone Visual Cryptography”, IEEE Tans. On Image Processing,vol.15, No.8, August 2006, pp. 2441-2453.
13. M.Naor and A.Shamir, “Visual Cryptography”, in Proceedings of Eurocrypt 1994, lecture notes in computer science, 1994, vol.950, pp. 1-12.
14. Robert Ulichney, “The void-and-cluster method for dither array generation”, IS&T/SPIE Symposium on Electronic Imaging and Science, San Jose, CA, 1993, vol.1913, pp.332-343.
15. E.R.Verheul and H.C.A. Van Tilborg, “Constructions and properties of k out of n visual secret sharing scheme”, Designs, Codes, and Cryptography, vol.1, no.2, 1997, pp.179-196.
16. ANSI, ANSI X9.44: Key Management Using Reversible Public Key Cryptography for the Financial Services Industry. Working Draft.
17. M. Bellare and P. Rogaway. Optimal Asymmetric Encryption-How to Encrypt with RSA. In Advances in Cryptology-Eurocrypt ‘94, pp. 92-111, Springer-Verlag, 1994.
18. M. Bellare and P. Rogaway. The Exact Security of Digital Signatures-How to Sign with RSA and Rabin. In Advances in Cryptology-Eurocrypt ‘96, pp. 399-416, Springer-Verlag, 1996.
19. D. Bleichenbacher. Chosen Ciphertext Attacks against Protocols Based on the RSA Encryption Standard PKCS #1. To appear in Advances in Cryptology-Crypto ‘98.
20. D. Bleichenbacher, B. Kaliski and J. Staddon. Recent Results on PKCS #1: RSA Encryption Standard. RSA Laboratories’ Bulletin, Number 7, June 24, 1998.

AUTHORS PROFILE

Sarita Rani, is pursuing her M.Tech (Optical Engineering) from Guru Jambheshwar University of Science & Technology, Hisar. She received her B.Tech (Electronics and Communication Enginering) from BRCM College of Engineering and Technology, Bahal, Bhiwani(MDU, Rohtak). Her area of interest is Image Processing.

Mamtesh Nokhwal, is pursuing her M.Tech (Optical Engineering) from Guru Jambheshwar University of Science & Technology, Hisar. She received her B.Tech (Electronics and Communication Enginering) from BRCM College of Engineering and Technology, Bahal, Bhiwani(MDU, Rohtak). Her area of interest includes Optoelectronics Instrumentation, Image Processing and MOMES-MEMS.

Dr Ajay Shankar, is an Assistant Professor at Guru Jambheshwar University of Science & Technology, Hisar under department of Optical Engineering(Applied Physic). He received his Phd (Physic) from IIT Dehli. He has 15 years of R & D experience in various industries in field of Optical Instrumentation. He has published more than 10 technical papers published in national journals and presented in seminars. His area of interests include Optical Instrumentation in field of Lens Designing and Image Processing .