International Journal of Computer Science and Network (IJCSN)
Volume 1, Issue 2, April 2012 www.ijcsn.org ISSN 2277-5420

A Novel Authenticity of an Image Using Visual Cryptography

[1] Prashant Kumar Koshta, [2] Dr. Shailendra Singh Thakur

[1] Dept of Computer Science and Engineering, M. Tech. Fourth Semester,
RGPV Bhopal- 462 036,Madhya Pradesh , India

[2] Dept of Computer Science and Engineering, GGCT Jabalpur - 482001,
Madhya Pradesh, India

Abstract
A digital signature is an important public-key primitive that performs the function of conventional handwritten signatures for entity authentication, data integrity, and non-repudiation, especially within the electronic commerce environment. Currently, most conventional digital signature schemes are based on mathematical hard problems. These mathematical algorithms require computers to perform the heavy and complex computations to generate and verify the keys and signatures. In 1995, Naor and Shamir proposed a visual cryptography (VC) for binary images. VC has high security and requires simple computations. The purpose of this thesis is to provide an alternative to the current digital signature technology. We introduce a new digital signature scheme based on the concept of a non-expansion visual cryptography. A visual digital signature scheme is a method to enable visual verification of the authenticity of an image in an insecure environment without the need to perform any complex computations. We proposed scheme generates visual shares and manipulates them using the simple Boolean operations OR rather than generating and computing large and long random integer values as in the conventional digital signature schemes currently in use.

Keywords: Digital signature scheme, Visual cryptography, RSA signature, DSA signature, Boolean OR operation.

I. INTRODUCTION

Information security in the present era is becoming very important in communication and data storage. Data transferred from one party to another over an insecure channel (e.g., Internet) can be protected by cryptography. The encrypting technologies of traditional and modern cryptography are usually used to avoid the message from being disclosed. Public-key cryptography usually uses complex mathematical computations to scramble the message.

A digital signature (DS) can provide the function of a conventional handwritten signature for the goals of entity authentication, data integrity, and non-repudiation . DS is an important method in public-key (asymmetric) cryptography. In 1976, Diffie and Hellman [1] first introduced the concept of digital signature, which is a verification scheme that concentrates on data authenticity [2], [3]. Most current digital signature schemes are based on mathematical algorithms that require very complex mathematical computations [3]. Therefore, the sender (signer) has to depend on a computer to digitally sign a document. Also, the receiver (verifier) has to use a computer to check the validity of the signature. Until now, building a digital signature scheme with high security and without complex mathematical computations has been a great challenge.

In 1997, Naor and Pinkas suggested new methods for visual authentication and identification of electronic payments based on visual cryptography (VC) . VC is a completely secure cryptographic paradigm that depends on the pixel level. It is an intuitive, easy-to-use method for encrypting private data such as handwritten notes, pictures, graphical images, and printed text after changing it to an image. VC uses the human visual system to decrypt the secret image from some overlapping encrypted images (referred to as shares printed on transparencies) without any complex decryption algorithms or the aid of computers. Hence, it can be used by anyone with or without knowledge of cryptography and without performing any cryptographic computations .

A new approach to digital signatures that is based on a non-expansion visual cryptography to overcome the disadvantage of the complicated computations required in current digital signature schemes.

In section II, we describe conventional digital signature schemes. Section III provides background in visual cryptography. In Section IV, we explain our new proposed signature scheme and Section V is the conclusion.

II. Conventional Digital Signature Schemes

Digital signature (DS) is the most effective technique for ensuring authentication, integrity, and non-repudiation of data in an open network such as the Internet . DS is a verification method requires the signature holder to have two keys: the private-key (signature key) for signing a message and the public-key (verification key) for verification of authenticity of the message (see Fig.1).

The main goal of DS is to verify that a message has not been modified in transit after it was signed and also, to give the receiver of the message confidence that it was sent by the expected party .The theory of the DS algorithm was first introduced by Diffie and Hellman in 1976 . However, the first practical system was the RSA digital signature scheme developed by Rivest et al. in 1978 [4]. Subsequently, DS schemes such as ElGamal signature [5], [6], undeniable signature [7] and others were proposed.

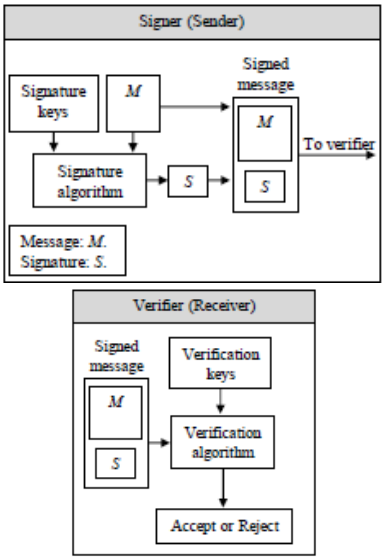

Fig. 1. The digital signature scheme

Most of the current DS schemes in use are based on the difficulty to solve complex mathematical problems. The most complex mathematical problems used for designing a signature scheme are integer factorization, such as the RSA digital signature scheme, and discrete logarithms, such as the Digital Signature Algorithm (DSA) [8]–[9].

A. The RSA digital signature scheme

RSA in general, is a public-key algorithm that is currently being implemented worldwide for key exchange, encryption, and digital signatures [5]. The RSA digital signature algorithm uses a private key for signing the original message and a public key for verification [8]. Fig. 2 shows the RSA digital signature scheme, in which a signed message is sent to the receiver (the verifier). On the receiver's side, to verify the contents of the received message, the verifier computes a new value (verification value) from the signed message and the signer's public key. Next, the verifier compares the verification value with the received message value. If the two values are identical, then the original message is verified and authenticated; if not, the signature is failed. The security of the RSA digital signature is based on the difficulty to compute integer factorization problem [8], [9].

Key Generation	
Select p, q	p and q both prime , $p \neq q$
Calculate $n = p \times q$	
Calculate $\Phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\Phi(n), e) = 1 ; 1 < e < \Phi(n)$
Calculate d	$d \equiv e^{-1} \pmod{\Phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

Encryption	
Plaintext :	$M < n$
Ciphertext :	$C = M^e \bmod n$

Decryption	
Ciphertext :	C
Plaintext :	$M = C^d \bmod n$

The DSA digital signature scheme

In 1991, the digital signature algorithm (DSA) was proposed by the U.S. National Institute of Standards and Technology (NIST) and became a United States Government Federal Information Processing Standard (FIPS) called the Digital Signature Standard (DSS) . Fig. 3 shows the digital signature algorithm (DSA), which is based on the ElGamal and Schnorr signature schemes. Both of these signature schemes are based on the same complex mathematical problem, namely, the discrete logarithms problem [3], [10]. The security of DSA is based on the complexity of the discrete logarithm problem in the field of Zp, where p is a prime [9].

Global Public Key components

p prime number where $2^{L-1} < p < 2^{L}$
for 512 <= L <= 1024 and L multiple of 64;
q prime divisor of(p-1), where $2^{159} < q < 2^{160}$;
g $= h^{(p-1)/q} \bmod p$,
where h is any integer with $1 < h < (p-1)$
such that $h^{(p-1)/q} \bmod p > 1$

User's Private Key

x random or pseudorandom integer with $0 < x < q$

User's Public Key

$y = g^{x} \bmod p$

User's Per-Message secret number

k = random or pseudorandom integer with $0 < k < q$

Signing

$r = (g^{k} \bmod p) \bmod q$
$s = [k^{-1}(H(M) + xr)] \bmod q$
Signature = (r,s)

Verifying

$w = (s')^{-1 \bmod q}$
$u1 = [H(M')w] \bmod q$
$u2 = (r')w \bmod q$
$v = [(g^{u1} y^{u2}) \bmod p] \bmod q$
TEST : v = r'

III. VISUAL CRYPTOGRAPHY

Visual cryptography (VC) is a powerful technique for sharing and encrypting images. Its value is that it is easily decoded visually by humans without knowing cryptography and cryptographic computations,[11]–[14]. In other words, visual cryptography is a concept that does not need any computational device to decrypt an encoded image [13], [14]. The simplest model of visual cryptography is called Naor and Shamir's (2, 2) visual cryptography scheme, which assumes that the original secret image is encrypted into two shadow images called transparent shares. Each pixel in the original secret image is encoded into 4 subpixels on every shadow image (transparent share) as shown in Table I. The original secret image can be decrypted by the human visual system when these two transparent shares are stacked together and the subpixels carefully aligned, where each share of these two shares looks like noise when inspected individually and reveals no information about the original secret image [11], [12], [15]. Fig 4 shows an example of implementing Naor and Shamir's (2, 2) scheme.

TABLE I
NAOR AND SHAMIR'S (2, 2) VISUAL CRYPTOGRAPHY SCHEME OF BLACK AND WHITE PIXELS WITH FOUR SUBPIXELS

Pixel of the secret image	White pixel		Black pixel	
Share 1				
Share 2				
Stacked results (Share 1+ Share 2)				

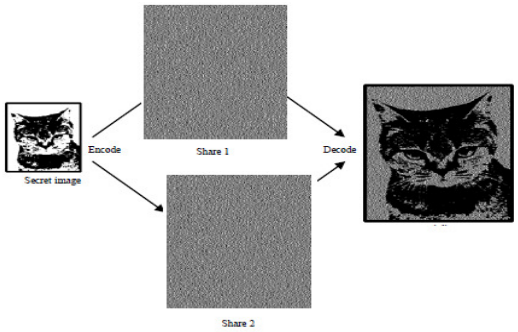

Fig. 4. Demonstration of Naor and Shamir's (2, 2) visual cryptography scheme with four subpixels

Most visual cryptography methods are based on the technique of pixel expansion; therefore, the resultant shares of encrypted secret image by this method are expanded several times of the original size thereby causing many problems such as image distortion, use of more memory space, and difficulty in carrying shares [16]. To overcome the problems resulting from the pixel expansion.

Yang [17] proposed a new visual cryptography method without pixel expansion for various cases such as (2, 2), (2, n), (k, k), and the general (k, n) schemes. He used the abbreviation ProbVSS (Probabilistic Visual Secret Sharing) to denote his method. In this method, a black and white secret image is encrypted into the same size shares as the secret image. In other words, instead of expanding the pixel into m subpixels as used in most visual cryptography methods, Yang's visual cryptography method uses one pixel to represent one pixel. That is, the size of the original image and shares (shadow images) are the same. Each pixel in the original secret image is represented as a black or white pixel in the shadow images without pixel expansion and the original secret image can be recovered by stacking and aligning carefully the pixels of these shares. ProbVSS method uses the frequency of white pixels in the black and white areas of the recovered image to let human visual system recognizes between black and white pixels. Also, this method uses the term "probabilistic" point out that our eyes can recognize the contrast of the recovered image based on the differences of frequency of white color in black and white areas. The contrast of this method is defined as $\alpha = p0 - p1$, where p-0 and p1 are the appearance probabilities of white pixel in the white and black areas of recovered image. Table II

shows Yang's (2, 2) ProbVSS scheme that a pixel on a black and white secret image is mapped into a corresponding pixel in each of the two shares. The secret image is recovered by stacking and aligning carefully the pixels of the two shares, where every pixel in share 1 is superimposed on the corresponding pixel in share 2; this is performed through the OR operation on the two transparent shares. Fig 5 shows an example of implementing Yang's (2,2)ProbVSSscheme.

TABLE II
THE (2, 2) VISUAL CRYPTOGRAPHY SCHEME OF BLACK AND WHITE PIXELS WITHOUT PIXEL EXPANSION

Pixel of the secret image	Share 1	Share 2	Recovered results	Probability
□	□	□	□	$p_0 = 0.5$
	■	■	■	$p_0 = 0.5$
■	□	■	■	$p_1 = 0$
	■	□	■	$p_1 = 0$

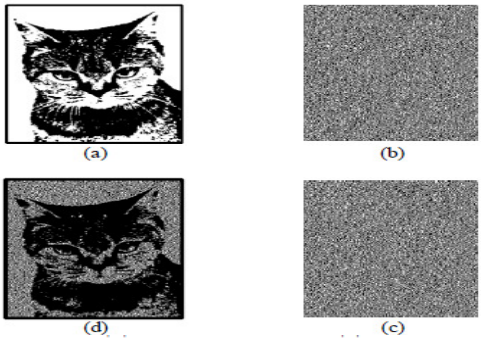

Fig. 5. The (2, 2) ProbVSS scheme: (a) The secret image, (b)The first share, (c) The second share, (d) The recovered image by stacking shares (b) and (c)

IV THE PROPOSED SCHEME

This propose scheme, a new approach to the digital signature scheme based on a non-expansion visual cryptography. In addition, the proposed scheme can work with or without the aid of computing devices. Boolean operation OR is used in the generation of our proposed scheme. The OR Boolean operation works for binary inputs as follows:

$$0 \vee 0 = 0, 0 \vee 1 = 1, 1 \vee 0 = 1, 1 \vee 1 = 1.$$

The OR operation of two N Row × N Column matrices, A and B, can be described by the following formulas:

$$\forall\, a_{ij} \in A, b_{ij} \in B,$$
$$C = A \vee B = \left[a_{ij} \vee b_{ij}\right], i = 1, \ldots, N_{Row}, j = 1, \ldots, N_{Column}.$$

The expression C = A V B means that the ij-th element, Cij of matrix C is equal to aij V bij where aij and b ij are the ij-th elements of matrix A and matrix B, respectively.

The new digital signature scheme use notations, which consists of three phases: initialization phase, signature phase, and verification phase.

A. The notations

Table III summarizes notations used in this paper.

TABLE III
THE NOTATIONS

Notation	Description
G	An integer number with
PU	A visual public share (common shadow image)
IM	A black and white secret image intended to be signed
PRs_i	The signer's visual private keys, where
PRv_i	The verifier's visual private keys, where
PUv	A verifier's visual public key
(R, S)	A visual signature pair generated by the signer
R	The first visual signature share of the visual signature pair (R, S) generated by the signer
S	The second visual signature share of the visual signature pair (R, S) generated by the signer
Cs_i	The first intermediate shares in the signature phase for generating the first visual signature share, R, of the visual signature pair (R, S), where
Cv_i	The first intermediate shares for generating the verifier's visual public key, PUv, where
Ds_j	The second intermediate shares in the signature phase for generating the first visual signature share, R, of the visual signature pair (R, S), where
Dv_j	The second intermediate shares for generating the verifier's visual public key, PUv, where
Es_i	The first intermediate shares in the signature phase for generating the second visual signature share, S, of the visual signature pair (R, S), where
Ev_i	The first intermediate shares in the verification phase, where
Fs_j	The second intermediate shares in the signature phase for generating the second visual signature share, S, of the visual signature pair (R, S), where
Fv_j	The second intermediate shares in the verification phase, where
V	A visual verification share generated by the verifier
	A complement of the visual verification share generated by the verifier
Bs	A full black share (binary matrix) with all elements (pixels) are ones (blacks)

B. Initialization phase

The proposed scheme involves two parties, the signer such as Alice and the verifier such as Bob.

- Alice and Bob agree on a public integer, G, with $G \geq 2$and a visual public share (common shadow image), PU, in the form of $n \times n$ pixels.
- Alice randomly and secretly generates G+1 visual private keys (shares), denoted by $PRs_1,\ldots, PRs_{G+1}$, where each one is in the form of $n \times n$ pixels.
- Bob randomly and secretly generates G+1 visual private keys (shares), denoted by $PRv_1,\ldots, PRv_{G+1}$, where each one is in the form of $n \times n$ pixels.
- Bob generates his visual public key, PUv, as follows:

First, he generates the first intermediate shares ($Cv_1,\ldots, Cv_G$) of G, as follows:

$$Cv_i = PRv_i \; V \; PU \qquad (i = 1,\ldots\ldots, G) \qquad (1)$$

Second, he generates the second intermediate shares ($Dv_1,\ldots, Dv_G$) of G, as follows:

$$Dv_j = PRv_{G+1} \; V \; Cv_j \qquad (j = 1,\ldots\ldots..,G) \qquad (2)$$

Third, he gets the visual public key, PUv, from the second intermediate shares ($Dv_1,\ldots, Dv_G$) of G, as follows:

$$PUv = Dv_1 \; V\ldots.. \; V \; Dv_G \qquad (3)$$

Fourth, he sends the visual public key, PUv, to Alice (the signer).

C. Signature phase

Note that, if the signer (Alice) wishes to send the image IM confidentially, she can use any existing encryption methods. To sign the image IM in the currently proposed scheme, Alice (the signer) performs the following steps:

1. She generates the first visual signature share, R, of the visual signature pair (R, S), as follows:

   First, she generates the first intermediate shares ($Cs_1,\ldots, Cs_G$) of G, as follows:

   $$Cs_i = PRs_i \, \mathrm{V} \, PU \qquad (i = 1,\ldots\ldots,G) \qquad (4)$$

   Second, she generates the second intermediate shares ($Ds_1,\ldots, Ds_G$) of G, as follows:

   $$Dsj = PRsG+1 \, \mathrm{V} \, Csj \qquad (j = 1,\ldots\ldots,G) \qquad (5)$$

   Third, she gets the first visual signature share, R, of the visual signature pair (R, S), from the second intermediate shares ($Ds_1,\ldots, Ds_G$) of G, as follows:

   $$R = Ds_1 \, \mathrm{V} \, \ldots\ldots \, \mathrm{V} \, DS_G \qquad (6)$$

2. She generates the second visual signature share, S, of the visual signature pair (R, S), as follows:

   First, she generates the first intermediate shares ($Es_1,\ldots, Es_G$) of G, as follows:

   $$Es_i = PRs_i \quad \mathrm{V} \quad PUv \quad (i = 1,\ldots\ldots,G) \qquad (7)$$

   Second, she generates the second intermediate shares ($Fs_1,\ldots, Fs_G$) of G, as follows:

   $$Fs_j = IM \quad \mathrm{V} \quad ES_j \qquad (j = 1,\ldots\ldots,G) \qquad (8)$$

   Third, she gets the second visual signature share, S, of the visual signature pair (R, S) from the second intermediate shares ($Fs_1,\ldots, Fs_G$) of G, as follows:

   $$S = Fs1 \, \mathrm{V} \, \ldots\ldots \mathrm{V} \, FsG \qquad (9)$$

Fourth, she checks visually whether R= Bs or S= Bs (full black shares); if not, proceeds to step 3; if yes; she repeats the following two steps until $R \neq Bs$ and $S \neq Bs$ (Not full black shares).

- She generates new visual private shares, $PRs_1,\ldots, PRs_{G+1}$.
- She performs steps 1 and 2.

3. She sends the visual signature pair (R, S) of IM to Bob (the verifier).

D. Verification phase

To verify that (R, S) is a valid visual signature of the image IM, the verifier (Bob) carries out the following steps: 1. He generates the visual verification share, V, as follows:

First, he generates the first intermediate shares ($Ev_1,\ldots, Ev_G$) of G, as follows:

$$Ev_i = PRv_i \; \mathrm{V} \; PRv_{G+1} \; \mathrm{V} \quad R \quad (i = 1,\ldots..,G) \qquad (10)$$

Second, he generates the second intermediate shares ($Fv_1,\ldots, Fv_G$) of G, as follows:

$$Fv_j = IM \, \mathrm{V} \; Ev_j \qquad (j = 1,\ldots,G) \qquad (11)$$

Third, he gets the visual verification share, V, from the second intermediate shares ($Fv_1,\ldots, Fv_G$) of G, as follows:

$$V = Fv_1 \, \mathrm{V} \, \ldots.. \, \mathrm{V} \, FV_G \qquad (12)$$

2. He checks whether V = S, as follows:
   First, he computes the complement of V (V is a binary

matrix "share"), denoted as , by replacing 0's with 1's and 1's with 0's.

Second, he gets the full black share, *Bs*, from superposition of and the signer's second visual signature share, *S*, as follows:

$$V' \vee S = Bs \qquad \textit{(Full black share)} \qquad (13)$$

If Equation (13) holds, the verifier (Bob) is convinced that (*R*, *S*), which is generated by Alice (the signer), is indeed the valid visual signature of the image *IM*. Consequently, Equation (13) is true only if V=S.

Fig. 6 shows the basic idea of the proposed scheme, namely, the Visual Digital Signature Scheme.

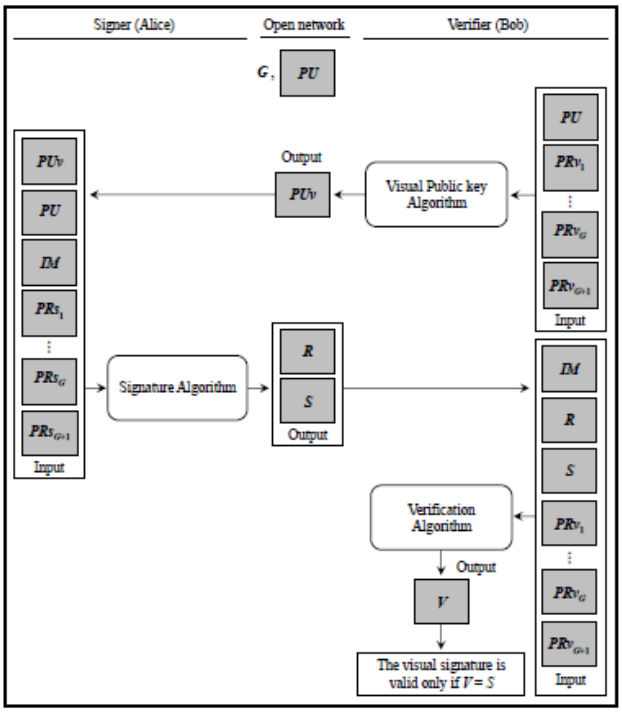

Fig. 6. The basic idea of the proposed scheme (Visual Digital Signature)

E. Comparison with famous current digital signature schemes

The proposed scheme has some advantages and benefits compared to conventional digital signature schemes. Table IV gives a summary of the comparison.

TABLE IV

BRIEF COMPARISON BETWEEN CURRENTLY FAMOUS DIGITAL SIGNATURE SCHEMES WITH THE PROPOSED SCHEME

Name of signature Scheme	Requirement	Secret information	Security condition	Complex computation
RSA	Computers	Numbers in finite fields	High	High
DSA				
ElGamal				
Our scheme	Human eye	Shadow images	Average	Low

V. CONCLUSION

In this paper, a new digital signature scheme was proposed, based on a non-expansion visual cryptography concept, namely, the visual digital signature scheme. Since only the simple Boolean OR operation was used to construct the scheme rather than complex computations used in current conventional digital signature schemes, the proposed scheme is easily implemented and has a specific niche in visual applications. The security of the scheme is based on the difficulty of solving and computing random Boolean OR operations, especially when using a large portion of the visual share and a large value for *G* (where *G* must be an integer with).

References

[1] W. Diffie, M. Hellman, "New Directions in Cryptography," IEEE Transactions in Information Theory, Vol. It-22, No. 6, 1976.

[2] M. Alia, "A new approach to public-key cryptosystem based on Mandelbrot and Julia fractal sets," Ph.D. thesis of the Universiti Sains Malaysia (USM), 2008.

[3] W. Stallings, Cryptography and Network Security-Principles and Practices, Prentice Hall, Inc, 4th Ed., 2006.

[4] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, Vol. 21, No. 2, pp. 120–126, 1978.

[5] C. S. Laih, K. Y. Chen, "Generating visible RSA public keys for PKI," Int. J. Secur., Vol. 2, No. 2, Springer, Berlin, 2004, pp. 103–109.

[6] ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Trans. Inform. Theory IT, Vol. 31, No. 4, pp. 469–472, 1985.

[7] C. David, H. V. Antwerpen, "Undeniable Signatures," Crypto'89, LNCS 435, Springer-Verlag, Berlin, 1990, pp. 212–216.

[8] MS, "Public Key Cryptography: Applications Algorithms and Mathematical Explanations," India, Tata Elxsi, 2007.

[9] M. Alia, A. Samsudin, "A New Digital Signature Scheme Based on Mandelbrot and Julia Fractal Seta," American Journal of Applied Sciences, AJAS, Vol. 4, No. 11, pp. 850–858, 2007.

[10] D. R. Stinson, Cryptography Theory and Practice, Chapman & Hall/CRT, 3rd Ed, 2006.

[11] J. A. Rodriguez, R. Rodriguez-Vera, "Image encryption based on phase encoding by means of a fringe pattern and computational

algorithms," Journal of Revista Mexicana De Fisica, Vol. 52, No. 1, pp. 53–63, 2006.

[12] T. Zohra, "Halftone Image Watermarking based on Visual Cryptography," M.S. Thesis of Electronics Science, Batna University, Republic of Algeria, 2005.

[13] S.F. Tu, C.-S. Hsu, "A VC-Based Copyright Protection Scheme for Digital Images of Multi-Authorship," The 2007 International Confernce of Signal and Image Engineering, U.K., 2007, pp. 685–689

[14] C.S. Hsu, S.-F. Tu, "Digital Watermarking Scheme with Visual Cryptography," The 2008 IAENG International Conference on Imaging Engineering,.

[15] C. Sung, C. Lo, C. Peng, W. Tasi, "A study on VOIP Security," Int. Computer Symposium, Taipei, Taiwan, pp. 15–17, 2004.

[16] C.S. Hsu, "A study of Visual Cryptography and Its Applications to Copyright protection Based on Goal programming and Statistics," Ph.D. Dissertation, National Central University, Taiwan, 2004.

[17] C.N. Yang, "New visual secret sharing schemes using probabilistic method," Pattern Recognition Letter, Vol. 25, pp. 481–494, 2004.

Prashant Kumar Koshta: was born in Jabalpur, MP India in 1982. He has completed his B.E. degree in Computer Science & engineering from Jabalpur Engineering Collage, RGPV(Bhopal), MP, India in 2005. He is student of Gyan Ganga Collage of Technology Jabalpur (MP) and presently pursuing M.Tech in Computer Technology and Applications. He is the IBM Certified Data Base Associate DB2. He is a Life Member of Computer Society of India. His area of Interest includes Data Structure, Algorithms, Complier Design and Computer Network and Data Communication He has published 4 papers in National & International Conferences ,one International journal and referred journals.

Dr. Shailendra Singh Thakur is a Professor in the Department Of Computer Science And Engineering, Gyan Ganga College of Technology, Jabalpur. He received his PhD in Computer Science in 2010 from Rani Durgawati Vishwavidyalaya, Jabalpur. He has published many research papers in various national and international journals. His areas of interest are Databases, Software Engineering and Network Security.