RESEARCH ARTICLE OPEN ACCESS

Digital Watermarking of Compressed Images with Improved Encryption

Aneena M
M.Tech
Department of Computer Science and Engineering
Lourdes Matha College of Science & Technology
Trivandrum
Kerala - India

ABSTRACT

Digital Image and information embedding systems have a number of important multimedia applications. These systems embed one signal, sometime called an "embedded signal" or "information" within another signal, called as "Host Signal". Digital image watermarking is a new approach, which is suitable for medical, military, and archival based applications. Unfortunately, watermarking techniques modify original data as a modulation of the watermark information and unavoidably cause permanent distortion to the original data. For some critical applications such as the law enforcement, medical and military image system, it is crucial to restore the original image without any distortions. The watermarking techniques satisfying those requirements are referred to as 'reversible watermarking'. Reversible, or lossless, watermarking is therefore required for many highly sensitive applications. To overcome this and to retrieve the original data, reversible watermarking has been implemented, which considered as a best approach over the cryptography. Reason being, it maintains the superlative property that the original cover can be listlessly recovered after embedded data is extracted while shielding the image content's privacy. The proposed method can achieve real reversibility that is data extraction and image recoveries are free of any error. An image based authentication along with visual cryptography is used to solve the problem of phishing.

Keywords:- Reversible watermarking, image captcha, visual cryptography, image encryption.

I. INTRODUCTION

Communication is one of the most important needs of human beings. For communication purpose, most of the people are using different devices like mobile phones, laptops etc. Most of these devices use certain network to make the communication easier. Device level security can be ensured by using facilities like setting passwords, biometric authentication schemes etc. But while coming to network level security the most important challenge that world faces today is to ensure data security. In the current trends of the world, the technologies have advanced so much that most of the individuals prefer using the internet as the primary medium to transfer data from one end to another across the world. There are many possible ways to transmit data using the internet: via emails, chats, etc. The data transition is made very simple, fast and accurate using the internet. However, one of the main problems with sending data over the internet is the security threat it poses i.e. the personal or confidential data can be stolen or hacked in many ways. Therefore it becomes very important to take data security into consideration, as it is one of the most essential factors that need attention during the process of data transferring. Data security basically means protection of data from unauthorized users or hackers and providing high security to prevent data modification. This area of data security has gained more attention over the recent period of time due to the massive increase in data transfer rate over the internet. Inorder to improve the security features data transfers over the internet, many techniques have been developed like cryptography, steganography and digital watermarking. Reversible watermarking in images is a

technique, by which the original cover can be losslessly recovered after the embedded message is extracted. This important technique is widely used in medical imagery, military imagery and law forensics, where no distortion of the original cover is allowed.

A.Digital Watermarking

The process of embedding the watermark into digital data is known as digital watermarking.It is the way of hiding secret message to provide data integrity and copyrights. Digital image watermarking is a new approach, which is suitable for medical, military, and archival based applications.The embedded watermarks are difficult to remove and typically imperceptible could be in the form of text,image or audio or video.

Basically there are four types of watermarking:

1) Text Watermarking: Text can be added into image is called text watermarking .

2) **Image Watermarking:** Image can be added into an original image is called image watermarking .

3) **Audio Watermarking:** Some audio signals are added into audio clip is called audio watermarking .

4)Video Watermarking: Some video signals are added into video clip

B.Visual Cryptography

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer. Naor and Shamir introduced the visual cryptography scheme (VCS) as a simple and secure way to allow the secret sharing of images without any cryptographic computations. They demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n − 1 shares revealed no information about the original image.

1)(2,2) Threshold VCS scheme: This is a simplest threshold scheme that takes a secret message and encrypts it in two different shares that reveal the secret image when they are overlaid. No additional information is required to create this kind of access structure.

In the case of (2, 2) VCS, each pixel P in the original image is encrypted into two sub pixels called shares.The choice of shares for a white and black pixel is randomly determined (there are two choices available for each pixel). Neither shares provide any clue about the original pixel since different pixels in the secret image will be encrypted using independent random choices.When the two shares are superimposed, the value of the original pixel P can be determined. If P is a black pixel, we get two black sub pixels; if it is a white pixel we get a white pixel as well as black pixel.

II. LITERATURE SURVEY

With regard to providing confidentiality for images, encryption is an effective and popular means as it converts the original and meaningful content to incomprehensible one. Although few data hiding techniques in encrypted images have been published yet, there are some promising applications that can be applied to encrypted images. In [9] Hwang et al. advocated a reputation-based trust-management scheme enhanced with data colouring (a way of embedding data into covers) and software watermarking, in which data encryption and colouring offer possibilities for upholding the content owner's privacy and data integrity. Obviously, the cloud service provider has no right to introduce permanent distortion during data colouring into encrypted data. Thus, a reversible data colouring technique based on encrypted data is preferred.

Reversible watermarking has found a huge surge of experimentation in its domain in past decade as the need of recovering the original work image after extracting the watermark arises in various applications such as the law enforcement, medical and military image system, it is crucial to restore the original image without any distortions [7]. In traditional watermarking techniques, our main concern is to embed and recover the watermark with minimum loss. The quality of original work image we get after extraction is highly degraded and not restorable. But in applications like law enforcement, medical and military, in which superior quality of image is needed, we cannot use these algorithms. In medical images, some prerequisite information about the patient is watermarked in it while transmitting and at reception we need to have both, the original image and that information to be recovered lossless. This type of result is achievable by making use of any reversible watermarking algorithm out of a pool of algorithms [8]. W. Puech et al. [2] proposed an analysis of the local standard deviation of the marked encrypted images in order to remove the embedded data during the decryption step for protection of multimedia based on Encryption and watermarking algorithms. These algorithms rely on the Kirchhoff's principle, details of the algorithm are known, and only the key for data encryption and data decryption should be secret. The first one is when there is homogeneous zones all blocks in these zones are encrypted in the same manner. The second problem is that block encryption methods are not robust to noise. Indeed, because of the large size of the blocks the encryption algorithms per block, symmetric or asymmetric cannot be robust to noise. The last problem we face is data integrity. The combination of data-hiding and encryption can solve these types of problems hence by using this approach a reversible data hiding method for encrypted images is able to embed data in encrypted images and then to decrypt the image and to rebuild the original image by removing the hidden data. But it is not possible to use when high capacity reversible data hiding method.

III. EXISTING METHODS

In previous methods of data hiding by first extracting compressible features of original cover and then compressing them losslessly, spare space can be saved for embedding watermark. A more popular method is based on difference expansion (DE) , in which the difference of each pixel group is expanded, e.g., multiplied by 2, and thus the least significant bits (LSBs) of the difference are all-zero and can be used for embedding messages. Another promising strategy is histogram shift (HS), in which space is saved for data embedding by shifting the bins of histogram of gray values. The state-of-art methods usually combined DE or HS to residuals of the image, e.g., the predicted errors, to achieve better performance. With regard to providing confidentiality for images, encryption is an effective and popular means as it converts the original and meaningful content to incoceivable one. Due to the increasing use of images in internet for security purposes, it is essential to protect the confidential image data from unauthorized access and phishing. Advanced Encryption Standard (AES) is a well known block cipher that has several advantages in data encryption. However, it is not suitable for real-time applications.

In Vacating Room After Encryption (VRAE) framework, a content owner encrypts the original image using a standard cipher with an encryption key. After producing the encrypted image, the content owner hands over it to a data hider and the data hider can embed some auxiliary data into the encrypted image by losslessly vacating some space according to a data hiding key. Then a

receiver, maybe the content owner himself or an authorized third party can extract the embedded data with the data hiding key and further recover the original image from the encrypted version according to the encryption key.

IV. PROPOSED METHOD

Our proposed system uses the concept of reversible watermarking and improved visual cryptography .Reversible watermarking is a technique which is completely used to restore the original image**.** An image based authentication system based on visual cryptography has been added for phishing detection and prevention. It prevents password and other confidential information from the phishing websites. Secure server verification is done using visual cryptography. Dynamically generating the image captcha is one of the major advantage of the system. The framework of proposed system consist of the following ,Image captcha generation, encrypted image generation, data hiding, data extraction and image recovery. The image captcha generation consist of a registration phase and a login phase

Proposed System Architecture

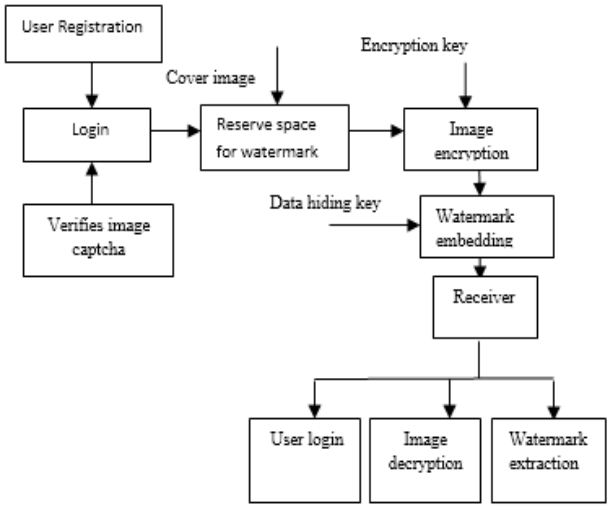

Fig 1.Architecture Of Proposed System

A.Image Captcha Generation

1) Registration phase

In the registration phase, a password or a key is asked from the user at the time of registration for the secure website. The key string can be a combination of alphabets and numbers to ensure more security. According to the key given by the user it is concatenated with randomly generated key in the server and an image captcha is generated such that the new image captcha is processed behind. Then "Blowfish Algorithm" is applied to divide the original image captcha into many blocks and rearranged.. There after the image captcha is split into two shares by (2,2) visual cryptography scheme such that it is divided according to black and white pixels. Then one of the share is kept with the user and the other share is kept with the server. The user's share and the original image captcha is sent to the user for later verification during login phase. The image captcha is also stored in the actual database of any confidential website as confidential data since the image captcha is used as the password later. After the registration, the user can change the key dynamically whenever it is needed. Registration process with sequence of encryption is depicted in Fig.2.

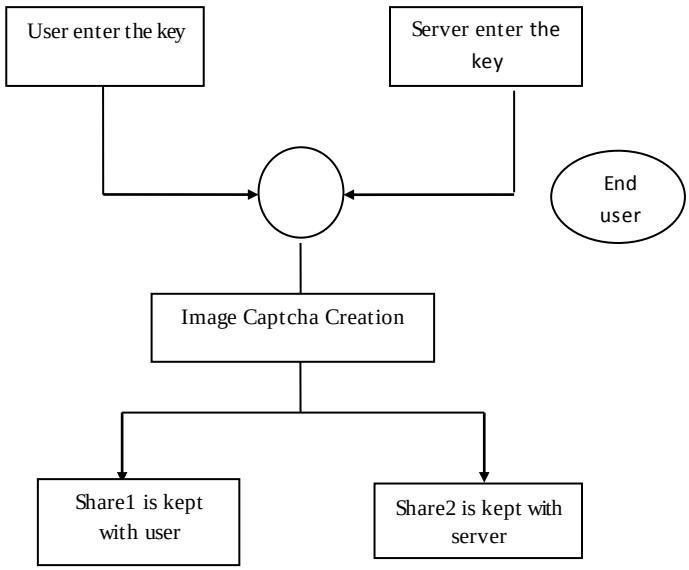

Fig.2 When user performs registration process for the website

2) Login phase

When the user logs in by entering his personal information for using his account, then first the user is asked to enter his username (user id) after that the user is asked to enter his share of image which is kept with him. This share is sent to the server where the user's share and server's share is stacked together to produce the image captcha. The generated image captcha is displayed to the user .Here the end user can verify whether the displayed image captcha matches with the captcha created at the time of registration. The end user needs to enter the text displayed in the image captcha and this can serve the purpose of

Password there by, the user can log into the website. By stacking two shares of username and image captcha one can verify whether the website is genuine/secure website or a phishing website and can also verify whether the user is a human user or not. This phase is depicted in Fig.3.

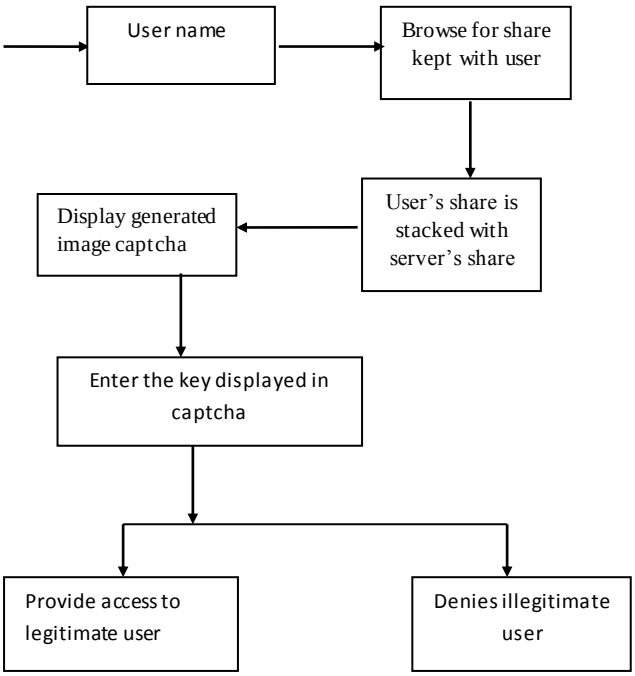

Fig 3.Login process

B.Encrypted Image Generation

Actually, to construct the encrypted image, the first stage can be divided into three steps: image partition, self-reversible embedding followed by image encryption. At the beginning, image partition step divides original image into two parts A and B; then, the LSBs of A are reversibly embedded into B with a standard watermarking algorithm so that LSBs of A can be used for accommodating messages at last, encrypt the rearranged image to generate its final version

1) Image partition

The main goal of image partition is to find a smoother area B. To do that, without loss of generality, assume the original image C has M*N pixels. First, the sender extracts several overlapping blocks from the original image, along the rows. Number of overlapping blocks is determined by the size of the message to be embedded. For each block, find the first order smoothness by defining the following function.

$$f= \sum_{u=2}^{m} \sum_{v=2}^{N-1} \left| C_{u,v} - \frac{C_{u-1,v}+C_{u+1,v}++C_{u,v-1}+C_{u,v+1}}{4} \right|$$

Higher f relates to blocks which contain relatively more complex textures. The content owner, therefore, selects the particular block with the highest f to be A , and puts it to the front of the image concatenated by the rest part B with fewer textured areas, the sender can also embed two or more LSB-planes of A into B, which leads to half, or more than half, reduction in size of A. However, the performance of A, in terms of PSNR, after data embedding in the second stage decreases significantly with growing bit planes exploited

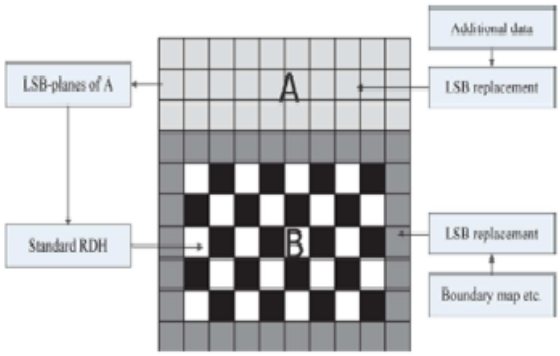

Fig 4.Illustration of Image partition and embedding process

2) Self-Reversible Embedding

The goal of self-reversible embedding is to embed the LSB-planes of A into B. Pixels in the rest of image B are first categorized into two sets: white pixels with its indices I and j satisfying (i + j) mod 2 = 0 and black pixels whose indices meet (i+j) mod 2 = 1, as shown in Fig 4,Then, each white pixel, $B_{i,j}$ is estimated by the interpolation value obtained with the four black pixels surrounding it as follows:

$$B'_{i,j}=w1B_{i-1,j}+w2B_{i+1,j}+ w3B_{i,j-1}+ w4B_{i,j+1}$$

where the weight Wi, $1 \leq i \leq 4$ .The estimating error is calculated via $e_{i,j=B_{i,j}-B'_{i,j}}$ and then some data can be embedded into the estimating error sequence with histogram shift. After that, we further calculate the estimating errors of black pixels with the help of surrounding white pixels that may have been modified. Then another estimating error sequence is generated which can accommodate messages as well. Furthermore, we can also implement multilayer embedding scheme by considering the modified B as "original" one when needed. In summary, to exploit all pixels of B, two estimating error sequences are constructed for embedding messages in every single-layer embedding process.

2) Image Encryption

After rearranged self-embedded image, denoted by X , is generated, we can encrypts X to construct the encrypted image denoted by E .With a block cipher (AES) the encryption version of X is easily obtained. Advanced Encryption Standard (AES) algorithm is used to carry out the final encryption. This algorithm is flexible in supporting any combination of data and key size of 128, 192, and 256 bits. With a stream cipher, the encryption version of X is easily obtained. For example, a gray value $X_{i,j}$ ranging from 0 to 255 can be represented by 8 bits

$X_{i,j}(0), X_{i,j}(1)\ldots X_{i,j}(7)$ such that

$$X_{i,j}(k)=\lfloor X_{i,j}/2^k \rfloor \bmod 2, \quad k= 0,1,....7 \quad (1)$$

The encrypted bits $E_{i,j}$ (k) can be calculated through exclusive or operation.

$$E_{i,j}(k) = X_{i,j(k)} \oplus r_{i,j}(k) \quad (2)$$

Where $r_{i,j}(k)$ is generated via a standard stream cipher determined by the encryption key. Finally, we embed 10 bits information into LSBs of first 10 pixels in encrypted version in order to tell data hider the number of rows and the number of bit-planes he can embed information into. After image encryption, the data hider or a third party cannot access the content of original image without the encryption key, thus privacy of the content owner being protected.

C. Data Hiding

The data hider can embed some data into the original A part .The Discrete Wavelet Transform (DWT) is

applied on the Luminance channel of color image, which produces the frequency subband coefficients. From these subband coefficients the highest texture energy subband is selected. On this subband apply *DWT* to obtain the second level decomposition. From this again select a subband having high texture energy. Before embedding the watermark into selected subbands, the watermark image is split into two shares by applying (2, 2) *V CS* scheme . Out of these two shares one share is embedded into selected subband and other share is kept secret.

1) Watermark Embedding Algorithm

1. Read the cover image I of size N × N and watermark image W of size M ×M

2. Decompose the color image into Luminance (Y), Intensity (I) and Hue (Q) channels of size M ×M

3. Split the watermark by applying VCS S0 is kept secret and S1 is used for embedding.

4. Apply DWT on Luminance (Y) channel to get subband coefficients (LL1, LH1, HL1 and HH1).

5. Extract the texture property Energy for each subband coefficient

6. Select the subband frequency coefficients (LL1 or LH1 or HL1 or HH1) which is having high energy.

7. Apply the DWT on selected subband to get second level decomposition (LL2, LH2, HL2 and HH2)

8. Extract the vector of texture property Energy for each subband of second level decomposition

9. Select the subband which is having high energy from second level decomposition (LL2,or LH2 or HL2 or HH2).

10. Embed the share S1 produced in Step 3 into the selected subband coefficients of Step 9 using following steps.

for i = 1 to M do

for j = 1 to M do

$Y\_(i, j) = (|Y(i, j)| + \alpha)S1(i, j)$

end for

end for

Where Y _(i, j) represents the modified frequency coefficient of subband, Y (i, j) represents the original frequency coefficient of subband, α represents the watermark scaling factor.

11. The value of α is adjusted such that the texture properties of embedded subband are changed by negligible value.

12 Replace the modified subband coefficients into its initial location and apply twice inverse DWT to get the watermarked Luminance channel.

13. Combine the watermarked Luminance (Y) channel with Intensity (I) and Hue (Q) to get watermarked color image.

D.Data Extraction and Image Recovery

1) Generating the Marked Decrypted Image

To form the marked decrypted image X" which is made up of A" and B" the content owner should do following two steps.

Step 1. With the encryption key, the content owner decrypts the image except the LSB-planes of A_E The decrypted version of E' containing the embedded data canbe calculated by

$X''_{i,j}(k) = E'_{i,j}(k) \oplus r_{i,j}(k)$ (3)

and

$X''_{i,j} = X''_{i,j}(k) \times 2^k$ (4)

where $E'_{i,j}(k)$ and $X''_{i,j}(k)$ are the binary bits of $E'_{i,j}$ and $X''_{i,j}$ obtained via (1) respoectively.

Step 2. Extract SR and ER in marginal area of B",By rearranging A" and B" to its original state, the plain image containing embedded data is obtained. The marked decrypted image X" is identical to rearranged X except LSB-planes of A . At the meantime, it keeps perceptual transparency compared with original image. More specifically, the distortion is introduced via two separate ways: the embedding process by modifying the LSB-planes of A and self-reversible embedding process by embedding LSB planes of A into B. The first part distortion is well controlled via exploiting the LSB planes of A only and the second part can benefit from excellent performance of current watermarking techniques.

2) *Watermark Extraction Algorithm*

Extraction algorithm is of type blind extraction which uses only watermarked color image as input. The watermarked color image is decomposed into Luminance, Intensity and Hue channels. The DWT is applied on the Luminance channel of watermarked color image, which produces the frequency sub band coefficients. From these subband coefficient the highest texture energy subband is selected. On this subband apply DWT to obtain the second level decomposition. From this again select a subband having high texture energy. The watermark is extracted from these selected subband coefficients. After extracting the watermark, the watermark image is superimposed with secret share using *VCS* scheme. The output of superimposition produces the extracted watermark. The details of the extraction algorithm is explained below.

Input : Watermarked (Color) image.

Output : Extracted watermark.

1. Read the watermarked color image I of size $N \times N$
2. Decompose the watermarked color image into Luminance (Y), Intensity (I) and Hue (Q) channels of size $M \times M$
3. Apply *DWT* on Luminance (Y) channel to get subband (*LL*1, *LH*1, *HL*1 and *HH*1).
4. Extract the texture property *Energy* for each subband coefficients.
5. Select the subband frequency coefficients (*LL*1 or *LH*1 or *HL*1 or *HH*1) which is having high energy.
6. Select the subband frequency coefficients (*LL*1 or *LH*1 or *HL*1 or *HH*1) which is having high energy.
7. Apply the *DWT* on selected subband to get second level decomposition (*LL*2, *LH*2, *HL*2 and *HH*2)
8. Extract the vector of texture property *Energy* for each subband of second level decomposition
9. Select the subband which is having high energy from second level decomposition (*LL*2,or *LH*2 or *HL*2 or *HH*2).
10. Embed the share $S1$ produced in Step 3 into the selected subband coefficients of Step 9 using following steps.

for $i = 1$ to M do

for $j = 1$ to M do

$Y\_(i, j) = (|Y(i, j)| + \alpha)S1(i, j)$

end for

Where $Y\_(i, j)$ represents the modified frequency coefficient of subband, Y (i, j) represents the original frequency coefficient of subband, α represents the watermark scaling factor.

11. The value of α is adjusted such that the texture properties of embedded subband are changed by negligible value

12. Replace the modified subband coefficients into its initial location and apply twice inverse DWT to get the watermarked Luminance channe

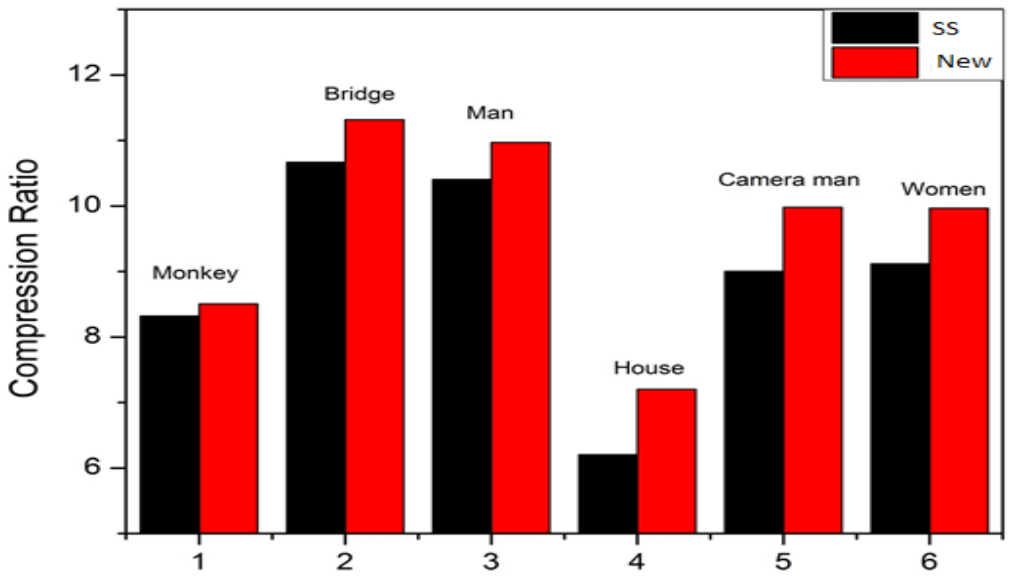

Fig5.Graphshowing dependency dynamics of compressed image

13. Combine the watermarked Luminance (Y) channel with Intensity (I) and Hue (Q) to get watermarked color image.

V. PERFORMANCE AND ANALYSIS

TABLE 1.Comparison Of Compression Ratios

Image Name	Compression Ratio after data Hiding by Spread Spectrum	Compression Ratio by our proposed method
Monkey	8.31935	8.305914
Bridge	10.66667	10.631679
Man	10.40342	10.370133
House	6.2029833	6.200885
Cameraman	9.001889	8.980032
Women	9.118364	9.965945

Our current techniques has been compared with data hiding method using spread spectrum.These diagrams clearly show the dependency dynamics of the compressed sequence quality from its size. Coordinates of the graph basic points are represented by the average PSNR values for the whole sequence and frame sizes. So each graph branch contains points that correspond to

different bit rates Each point on a graph represents difference between point on codec PSNR graph of SS and proposed and possibly interpolated PSNR value on this bit rate value.

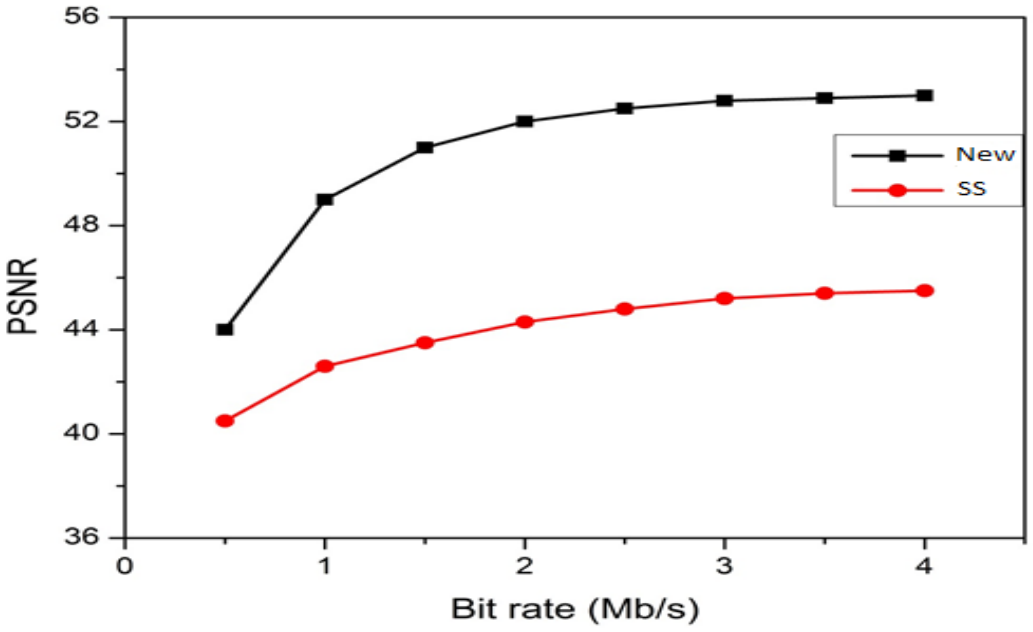

Fig 6.Graph showing PSNR

From the graph, it shows the proposed method have higher PSNR than the Spread Spectrum method.

VI. CONCLUSION

Reversible watermarking in encrypted images is a new topic drawing attention because of the privacy-preserving requirements from cloud data management this novel method can achieve real reversibility, separate data extraction and great improvement on the quality of marked decrypted images. The data hider can benefit from the extra space emptied out in previous stage to make data hiding process effortless. Achieve excellent performance without loss of perfect secrecy. Phishing websites as well as human users can be easily identified using our proposed system**.** This method provides additional security in terms of not letting the intruder log in into the account even when the user knows the username of a particular user.

REFERENCES

[1] Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption Kede Ma, Weiming Zhang, Xianfeng Zhao, Member, IEEE, Nenghai Yu, and Fenghua Li IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 3,MARCH 2013

[2] William Puech, Jose Rodrigues, Jean-Eric Develay-Morice. A New Fast Reversible Method for Image Safe Transfer. Journal of Real-Time Image Processing, Springer Verlag (Germany), 2007, 2

[3] Image Captcha Based Authentication Using Visual Cryptography IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 2, April-May, 2013 **ISSN: 2320 - 8791** www.ijreat.org

[5] J. Tian, "Reversible data embedding using a difference expansion,"*IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896, Aug. 2003.

[5] Lixin Luo, Zhenyong Chen, Ming Chen, Xiao Zeng, and Zhang Xiong, Reversible Image Watermarking Using Interpolation Technique IEEE TRANSACTIONS ON INFORMATION FORENSICS ANDSECURITY, VOL. 5, NO. 1, MARCH 2010

[6] L. Luo et al., " Reversible image watermarking using interpolation technique," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 187–193, Mar. 2010.

[7] J. TianPO, "Wavelet-based reversible watermarking for authentication," in Security and Watermarking of Multimedia Contents IV—Proc. SPIE, E. J. Delp III and P. W. Wong, Eds., Jan. 2002, vol. 4675, pp. 679–690.

[8] B. Macq, " Lossless multiresolution transform for image authenticating watermarking," in Proc. EUSIPCO , Sept. 2000, pp. 533–536.

[9] K. Hwang and D. Li, "Trusted cloud computing with secure resourcesand data coloring," IEEE Internet Comput., vol. 14, no. 5, pp. 14–22,Sep./Oct. 2010