An Integrated Message Hiding and Message Extraction Technique for Multimedia Content Using Invisible Watermarking Technique

M. Keerthika[1], Dr. S. Miruna Joe Amali [2]
[1]*PG Scholar, Department of Computer Science, KLN College of Engineering, Sivagangai, India*
2Associate Professor, Department of Computer Science, KLN College of Engineering, Sivagangai, India
keerthisugan90@gmail.com, joe.miruna@gmail.com

Abstract- The protection of multimedia data is becoming very important. The protection can be done with encryption. Involving both encryption and compression side-by-side needs more complex algorithms for content retrieval. Reconstructing the compressed encrypted content without much information loss is important. This work improves the ratio-distortion performance and also embedded message in the source image can be extracted for the source image authentication by using invisible watermarking technique. The message can be embedded into and extracted from the source image using watermarking techniques. The watermarked image is compressed by using quantization method to improve the compression ratio. The compressed image is encrypted and decrypted using modulo-256 addition by adding pseudo-random numbers into the image pixels. The encrypted image is splitted into number of files and in the user side using the auxiliary information (AI), file is merged using file adaptive wrapper method to decrypt the source image. Finally, with the use of verification key the embedded message is extracted and the source image is verified. It is shown that this method improves the ratio-distortion performance in compressing a watermarked image and better quality of reconstructed image. In order to further improve the distortion performance and quality of the reconstructed image other compression methods can be used.

Keywords—*Image Encryption and decryption, Image Compression, Auxiliary Information (AI) and Discrete Cosine Transform (DCT), Image Watermarking*

*****

I. INTRODUCTION

The data amount of cipher-text signals can be reduced without revealing the plaintext content and the encryption of compressed multimedia content is an evolving technology [1]. Security is an important issue in communication and storage of images, and encryption is one the ways to ensure security. Image encryption techniques try to convert original image to another image that is hard to understand. To keep the image confidential between users, decryption could not be done to know the

content without the key. The Slepian-Wolf theorem gives the lossless coding rate when some source side information is available at the decoder side but unavailable at the encoder side. For the encrypted multimedia compression, the cipher text signals can be viewed as the source, and the secret key and the estimate of plain text content as the side information [2]. The goal is to efficiently compress the cipher texts and to retrieve the plain texts from compressed data by exploiting the side information. The data amount of image grows day by day. It is quite costly
to store and transmit the image which requires large storage and bandwidth [3].To avoid the leakage of information modulo 256 additions is used by masking the original pixel values [4]. Hence image compression methods are necessary. The image compression techniques are categorized into two main classifications namely lossy compression techniques and Lossless compression techniques [8]. Lossless compression yields only less compression ratio but gives good quality of compressed images, whereas the lossy compression techniques lead to loss of data with higher compression ratio [6].

Compressing an image is different than compressing raw binary data. Of course, general compression programs can be used to compress images, but the result is less than optimal. This is because images have certain statistical properties which can be exploited by encoders specifically designed for them. Also, some of the finer details in the image can be sacrificed for the sake of saving a little more bandwidth or storage space. This also means that lossy compression techniques can be used in this area [5]. There are also two types of lossy compression methods for encrypted signals: compressive sensing based method and quantization based method.

This work proposes a novel scheme of compression, message hiding and message extraction for the images with the help of auxiliary information, watermarking and verification key. In watermarking phase, at the client side message is embedded using verification key [9]. In

 ISSN: 2321-8169
2702 - 2706

compression phase, the message embedded watermarked image is compressed in various DCT sub-bands are effectively compressed by using a quantization mechanism and an optimization method with ratio-distortion is employed to select the quantization parameters. In the encryption phase, the compressed image is encrypted by adding pseudo-random numbers into the pixels and employs one by one modulo-256 addition into the pixels. The encrypted image is splitted and AI is generated and transferred. At a user side, splitted file is merged by using AI and file adaptive wrapper method. The original message is extracted from the merged file and image is verified by using a verification key [7]. The result shows the ratio-distortion performance of the proposed work is significantly better than that of existing techniques and the image and message extracted is verified for the authentication of original image.

II. SCOPE OF THE PROJECT

The main scope of this work is to improve the ratio-distortion performance and extracting the embedded message from the watermarked image for original image verification and the computational complexity is also reduced. In the proposed work, to get an encrypted image the content owner firstly masks all pixel values in original compressed watermarked image and provides the encrypted data to split into number of files. The splitted file along with the AI is transferred and at the user side with the help of AI splitted file is merged. Embedded message is extracted from the merged image file by using a verification key which is already used to embed a data in a original image. A sketch of the proposed work is presented in Figure 1.

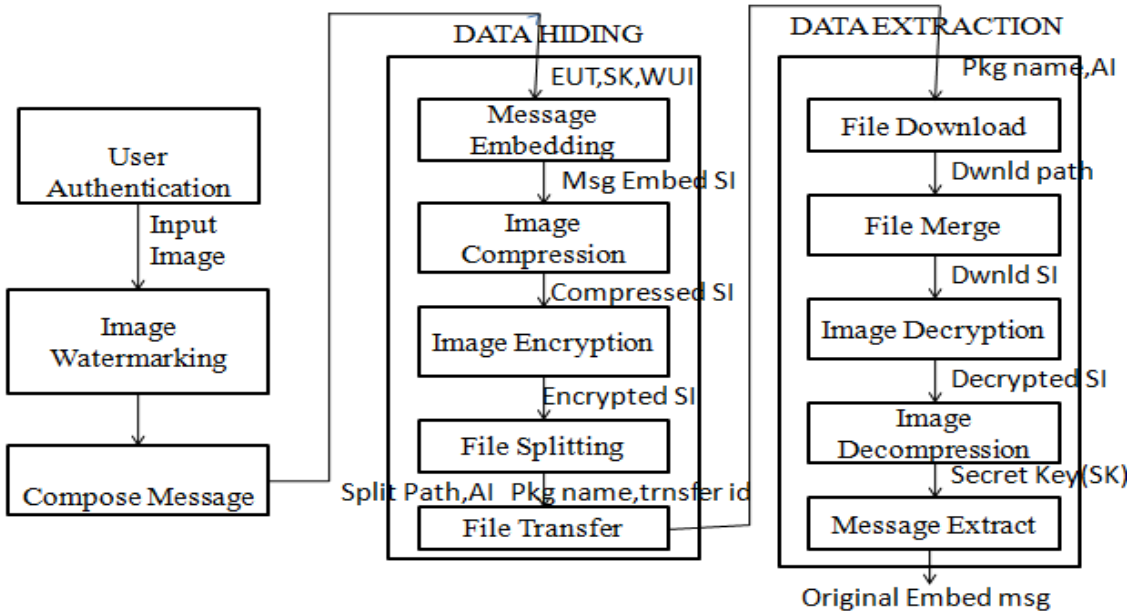

Figure1. Sketch of the proposed work

III. METHODOLOGY USED

3.1 IMAGE WATERMARKING

In the invisible image watermarking technique, the information embedded stamped image $I'(i,j)$ is produced when a binary map $b(i,j)$,of an watermark image $W(i,j)$,is embedded into the source image, $I(i,j)$.The processing takes place with each pixel in the source image and to the selected pixel watermark extraction function $WX(*)$ is applied. The extracted watermark value obtained is tested to determine whether it is equal to the desired watermark value. This process proceeds to the next pixel if the extracted watermark value is equal to the desired watermark value. If they are not equal, the selected pixel value is changed until the extracted watermark value is equal to the desired value. To produce small and random changes pixel values are modified. Using a modified error diffusion procedure, modification amount is calculated and then propagated to pixels

Which are not yet processed. This process is repeating until each pixel in the source image has been processed. With the information embedded stamped image, verification key is produced as the final products. By using this verification key, the watermark extraction function is calculated. The verification key may be in the form of three sets of binary look-up-tables (LUT) for a color image and can be

ISSN: 2321-8169
2702 - 2706

generated by using a Pseudo-random-number generator. Three sets followed by one for each color component and a single LUT for a gray-scale image. Using the below mentioned expression watermark extraction function $WX(*)$ is formed by combining LUTs

$$b(i,j) = LUT\mathcal{R}(IR(i,j)) \oplus LUTG(IG(i,j)) \oplus LUTB(IB(i,j))$$

Where $\oplus$ represents for a color image and $b(i,j) = LUT(l(i,j))$ for a monochrome image. If the desired watermark value does not match with the watermark value extracted from a given image pixel. The alteration of pixel values is needed until the watermark values match the given set of LUTs.

3.2 IMAGE COMPRESSION

The compression procedure is as follows. The compression will be performed in 64 DCT sub-bands with different quantization parameters. The channel provider firstly implements 2D DCT in the encrypted image with a block by block manner and then reorganizes the coefficients in each sub-band as a vector. After that, perform orthogonal transform for the vectors.

By using the orthogonal transform, there construction error will be uniformly scattered over all the DCT coefficients in a same sub-band, leading to a reconstruction result with better visual quality. Channel provider collects a down sampling image of the encrypted version.

3.3 IMAGE ENCRYPTION

The content owner encrypts the original image by adding pseudo-random numbers into the pixels. The content owner generates the auxiliary information according to the original and encrypted content and provides it to the channel provider.

Assume the original image is in compressed format and the pixel values are within [0,255]. Denote the numbers of the rows and the columns in the original image as N1 and N2, and the number of all pixels as$N(N = N1 * N2)$ implying that the bit amount of original image is 8.N. The content owner pseudo-randomly generates integers uniformly distributed within [0,255], and employs a one-by-one addition modulo 256 to produce an encrypted image,

$$c(i,j) = mod[p(i,j) + k(i,j), 256], \quad 1 \le i \le N1, 1 \le j \le N2$$

Here, p (i, j) are the gray values of pixels at positions (i, j), k (i, j) are the pseudo-random numbers derived from a secret key, and c (i, j) are the data of encrypted image. Clearly, the values of c (i, j) also obey a uniform distribution within [0,255]. An attacker without the knowledge of secret key cannot reveal the image content.

If the bandwidth is enough, any other operation is needless. We assume both N1 and N2 are multiples of 8.The content owner generates a down sampling sub-image with a size of N1/8 * N2/8,

$$pd(i,j) = p(8i, 8j)\ 1 \le i \le \frac{N1}{8}, 1 \le \le \frac{N2}{8}$$

and estimates the values of the pixels according to the sub image using a bilinear interpolation method. The pixel values in the interpolated image are denoted as $g(i,j)$. Then, the content owner divides the original and interpolated images into a number of blocks sized 8*8 and performs 2D discrete cosine transform in each block, where DCT means the 2D discrete cosine transform. With viewing the coefficients as 64 sub-bands, the content owner calculates the square roots of the average interpolation distortion in each sub-band.

The content owner also calculates a binary map $s(i,j) = \left\lfloor p(i,j) + \frac{k(i,j)}{256} \right\rfloor \oplus \left\lfloor g(i,j) + \frac{k(i,j)}{256} \right\rfloor$

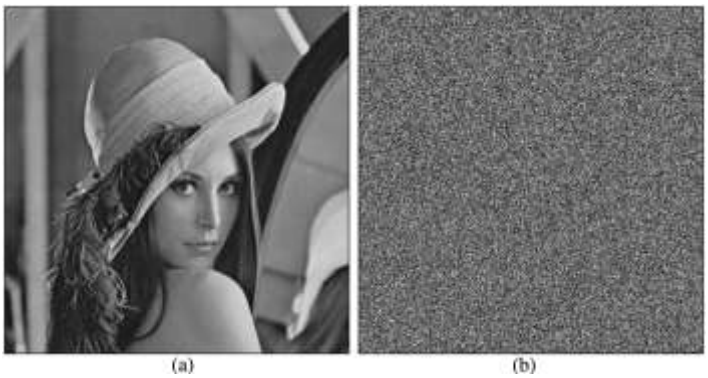

Figure 2. (a) Original image Lena and (b) its encrypted version

The original image and its encrypted version shows in Fig.2.Since the interpolated version $g(i,j)$ is similar to the original image$p(i,j)$, most of $s(i,j)$ are 0 and the rest, a small portion of $s(i,j)$, are 1.So, the data amount of $s(i,j)$ can be significantly reduced by lossless compression. The compressed version $s(i,j)$ is also encrypted and the encrypted compressed $s(i,j)$ is regarded as the second part of auxiliary information.

3.4 IMAGE FILE SPITTING AND MERGING

Based on the encrypted image, Auxiliary information (AI) is generated. File adaptive wrapper is used for file splitting and merge mechanism. Encrypted sub image is splitted into

numbers oh chunks in a file. Splitted file is transferred along with the Package name, split path, Transfer id, AI. Transferred file can be downloaded by login into the valid id. Package can be reviewed and downloaded with the help of AI generated and transferred. Downloaded package can be merged in the same path

3.5 IMAGE DECRYPTION

With the compressed data and the secret key, a receiver can perform the following steps to reconstruct the original image. Decompose the merged data file to get the encrypted sub-image. Decrypt the sub-image $cd(i,j)$ to retrieve the original sub-image $pd(i,j)$, and obtain the interpolated image $g(i,j)$ from $pd(i,j)$ using the bilinear interpolation method. Also, retrieve the values of $s(i,j)$.Receiver can obtain an estimate of encrypted image,

$$c'(i,j) = p(i,j) + k'(i,j)$$

The receiver will modify the estimated encrypted image and after performing 2D DCT in a block-by-block manner and reorganizing the DCT coefficients in 64 sub-bands as 64 vectors, then perform inverse orthogonal transform and the inverse 2D DCT.

The reconstructed image is obtained

$$p'(i,j) = c'(i,j) - k'(i,j)$$

Figure.3. (a) Reconstructed Lena with compression size 215, and (b) another reconstructed version with compression ratio27.99.

Fig.3. Shows the compression size of reconstructed Lena image and the compression ratio of the original Lena image and the compressed Reconstructed Lena image.

3.6 MESSAGE EXTRACTION

Original image can be decrypted and message embedded can be retrieved by using the verification key. Encrypted message is decrypted and arranged. Original message is revealed and upon verifying the message extracted with the original message embedded, original image is authenticated.

IV. EXPERIMENTAL RESULTS

Table 1 below shows that the results of compression on various types and sets of images, it represents the size before compression and size after compression of the images.

Table 1: Compression Ratio

S.NO	File Name	File Type	Before Compression (Size)	After Compression (Size)	Compression Ratio (%)
1	Lena	bmp	768	600	78.12
2	Doll	jpeg	35.2	20.07	60.98
3	Fruits	jpeg	187	95	50.12

V. CONCLUSION

An image encryption/decryption and compression method based on a modulo 256 addition and quantization method. Message is embedded into the source image by using invisible watermarking techniques using a verification key and the same embedded message can be extracted from the image to check the source image. For the encryption, original compressed image is loaded and the client encrypts the source image by adding pseudo-random numbers into the pixels and the pixel values are within [0, 255].Now an encrypted image is splitted into number of files and merged using the transferred AI.

Finally, an original image is reconstructed with high quality by using secret key and it is shown that compression ratio of an encrypted image and the decryption performance of an original image is improved and the by using the message extracted from the image original image gets authenticated which provides more security in the image transmission.

ACKNOWLEDGMENT

The authors would like to thank the reviewers for their valuable comments that would help to improve this work further.

REFERENCES

[1] M. Johnson, P. Ishwar, V. M Prabhakaran, D. Schonberg, and K. Ramchandran, “On compressing encrypted data,” IEEE Transactions on Signal Processing, Volume 52, No 10, pp. 2992–3006, October 2004.

[2] R. S. Gamil, Qaid, N. Sanjay, Talbar, “Encryption and Decryption of Digital Image Using Color Signal,” IJCSI International Journal of Computer Science Issues, Volume 9, No 2, March 2012.

[3] D. Klinc, C. Hazayy, A. Jagmohan, H.Krawczyk, and T. Rabinz, “On Compression of data encrypted with block ciphers,” IEEE Transactions on Information Theory, Volume 58, No 11, November 2012.

[4] X. Zhang, G. Feng, Y. Ren, Z. and Qian, "Scalable coding of encrypted images," IEEE Transactions on Image Processing, Volume 21, No 6, pp. 3108–3114, June 2012.
[5] X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," IEEE Transactions on Information Forensics Security, Volume 6, No 1, pp. 53–58, 2011.
[6] R. Lazzeretti, and M. Barni, "Lossless compression of encrypted grey-level and color images," in Proceedings of 16th Europe Signal Processing Conference (EUSIPCO2008), August 2008.
[7] Vinita Gupta and Atul Barve "A Review on Image Watermarking and Its Techniques," International Journal of Advanced Research in Computer Science and Software Engineering, volume 4, No 1, and pp: 92-97, 2014.
[8] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," IEEE Transactions on Signal Processing, Volume 19, No 4, pp. 1097–1102, April 2010.
[9] Minerva M. Yeung and Mintzer, F, "An Invisible Watermarking Technique for Image Verification," IEEE International Conference on Image Processing, Volume 2, pp.680-683,Oct 1997.