AN EFFICIENT APPROACH OF SENSITIVE AREA WATERMARKING WITH ENCRYPTION SECURITY

Ankita Ojha
M.Tech. Scholar
CSE Department
LNCT, Bhopal

Tripti Saxena
Assistant Professor
CSE Department
LNCT, Bhopal

Dr.Vineet Richariya
HOD
CSE Department
LNCT, Bhopal

Abstract **- Recently in the field of watermarking there are lots of facilities in communication, transmission and changes of data or information. There are lot of digital watermarking techniques have been made and implemented to stop the illegal use of the digital multimedia images or data. Robust and reversible watermarking technique is one of them. In this paper, we propose a reversible visible watermark technique, which embeds data into images to create a watermark. This paper tries to simply calculate n1,n2,n3 three variable with the help of key to achieve the digital watermark without any complex calculations and calculate the PSNR ,robustness and capacity of colored image. A reversible watermarking technique is used to embed the watermarking data, which can be used to recover the main images, into the watermarked images.**

Index Terms— Authentication, Encryption, integrity, Security, Watermarking, .

I. INTRODUCTION

In recent year all the organization's business working environment are going for the digital era, due to the largest advancement in recent technologies like in the area of data transmission, networked multimedia system, cloud computing, digital signature etc. Also from the last few years use of internet is exponentially increased, in business environment towards achievement of convenience, reliability and Security by introducing the digital security in their work. This multimedia data includes text, pictures, video, audio and application software which are shared over public network, so that it's user responsibility to protect this multimedia data. Cryptography, data authentication, steganography and time stamping are some techniques which are used for data security. Also there is another technique that raised the security level of multimedia data by combining a low level signal directly into the multimedia data. These low level signals are known as watermark, that uniquely identities the owner of the digital data and provide the security to the digital data and can be easily extracted.

In cryptography, the process of encoding information in such a way that only authorized person can read it called as encryption. Encryption does not prevent hacking or intruding, but denies the message content to the hacker or intruder. In an encryption scheme, the message, referred to as plaintext, is encrypted with the help of encryption algorithm, generating cipher text that can only be read if decrypted.

Digital Watermarking is process of hiding the watermark information into a digital data. It is a way of embedding unremarkable labels or logos or pattern or information data into the digital data.

Digital watermarking is a new technique, which is good for bank, medical, military, business and authentication based applications. The hidden watermarks are very difficult to remove could be in the form of multimedia data like image, video or

audio, text. The hiding of secret watermark in multimedia data, It does not matter how much hidden it is. However it tends to few degradation and distortion in the resultant hidden multimedia data. For solving these type of problem and for retrieving the original data, reversible watermarking technique has been used, this is the best approach compared to cryptography. After encryption in cryptography the resultant data may not be seen or understood also at the time of accessing this may increase loss of information of sender data, which is not in case of digital watermarking. When several watermarks embedded in digital data at the same time then this is known as multiple watermarking techniques. A digital image watermarking also worked as digital signature which gives the authenticity.

Digital watermarking is of two main types, namely embedding process and extracting process. In hiding process, watermark is hidden into the digital information. The original digital information will slightly modified after embedding the watermark, this modified information is called as watermarked information. While in accessing process this hidden watermark is accessed from the watermarked information and retrieve the original digital information. After comparing the accessed watermark to the original watermark; if the retrieve watermark is found same it gives authenticated data. During the transmission of the watermarked information over the public network hacker may hack the information, and if any changes in the information can be identified by comparing the accessed watermark with the original watermark.

There are two types of watermarking:

Visible watermarking: If we can see the information in the picture or video then this type of watermarking is known as visible watermarking. Generally, the data is in the form of text or a logo which identifies the owner of the digital media; this is also a visible watermark.

Invisible Watermark: In invisible watermarking, watermark is added as digital data to multimedia data such as audio, picture, video but it cannot be perceived. Database watermarking is the example of this category.

II. RELATED WORK

To improve the quality of the image different researchers proposed various approaches. In this section literature of the related work is discussed. The first reversible watermarking scheme for relational databases was proposed in. In this technique, histogram expansion is used for reversible watermarking of relational database. Zhang et al. proposed a method of distribution of error between two evenly distributed variables and selected some initial nonzero digits of errors to form histograms.

In 2014, Bajaj, A.[2] gives a advanced technique for Robust and reversible digital image watermarking technique. This technique is generally worked on the principle of RDWT-DCT-SVD. Hybrid image watermarking technique takes advantages of different transforms like RDWT, DCT, and SVD.

This algorithm is worked on different type of host images and different types of intensity watermarks. For measuring the correctness of this technique, the correlation based extraction mechanism is used . And PSNR is check to measured fidelity of watermarked and extracted original image.

In 2013, Saman Iftikhar, M. Kamran and Zahid Anwar[1] gives for Relational Data Robust and Reversible Watermarking Technique . In this paper, a semi-blind and robust reversible watermarking technique for numerical relational data has been introduced that manages Experimental studies prove the power of RRW against unauthorized attacks and compare result of the proposed technique from existing ones.

In 2014 Fujiyoshi, M.,[23] introduces a process for near-lossless data hiding. A data hiding process breaks an image to embed information in the image, and the process withdraw the hidden information from the distorted image. The introduced process also recovers an image from the distorted image where a pixel in the recovered image differs from the original one by not more than a pre-specified value. First in the introduced process, an image is quantized by nonuniform quantizer. Then, the histogram-based lossless DH process hides data to the quantized image.

In 2013,K. Jawad and A. Khan[4] proposed "For relational databases genetic algorithm and difference expansion based reversible watermarking," The main idea of this paper is based on difference expansion and utilizes genetic algorithm to increase watermark capacity and reduce distortion. This approach approach is reversible so that, distortion generates after watermark insertion can be fully recovered. With the help of GA, different attributes are identified to find the optimal criteria instead of selecting less effective attributes for watermark insertion. Searching the distortion tolerance of two attributes for a selected tuple may not be helpful for watermark distortion and capacity so that, distortion tolerance of different attributes are exposed. To predict watermarked attribute distortion created because of difference expansion can help an intruder. Thus, making it tough for an intruder to predict watermarked attribute or data we have tuple and attribute-wise distortion in the fitness function of GA,

In 2012 E. Sonnleitner[8], proposed "A robust watermarking approach for large databases" in which a watermarking algorithm that used a public watermark worked on partitioning, parameterized tuple and whitespaces. The watermarking scheme is non-intrusive, blind, reversible, resilient and applicable for databases of any size and type with right performance on embedding and extraction process. Moreover, we stressed out locatability of malicious changes within the scope of predefined tuple sets, and support incremental watermarking to overcome the dynamic nature which database systems are subjected to.

In 2012 J.-N. Chang and H.-C. Wu[5], proposed "Using difference expansion based on SVR prediction, reversible fragile database watermarking technology". By embedding the important characteristics of the real database it finds out database changes. Data mining is used to find out the relationship existing among the protected attributes and others in the database with the help of the association rule of frequent pattern tree. To predict each protected attribute value support vector regression (SVR) is used.

By the differences between the original and predicted values and applying difference expansion (DE) , the owner can place the digital watermark in the secured database. The SVR function predict the protected values after the protected database is distorted, Then, an inspection of the difference between original protected and predicted values we can find the digital watermark. FP-tree mining method is used for reducing SVR training time. When we extract digital watermark from the protected database and find the database has been changed with, then this method can use the find digital watermark to locate and authenticate the changed tuples.

III. PROPOSED METHOD

This method consists of two parts: embedding and extraction process. The proposed method is for the embedding data in images to provide security for information which we want to kept secret over an open channel. In this method we combined Encryption and Watermarking together. First we encrypt the data with the help of cryptography and after that encrypted data will be embedded in image by watermarking method. So the proposed method takes two steps for embedding process.

Fig.1 Original Lenna Image

Fig.2 Selected black area where digital Watermarking data reside

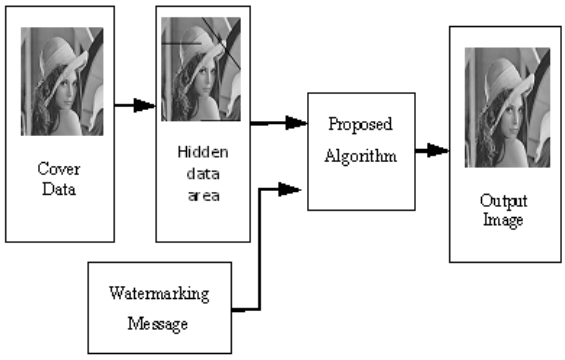


Fig.3 Proposed algorithm

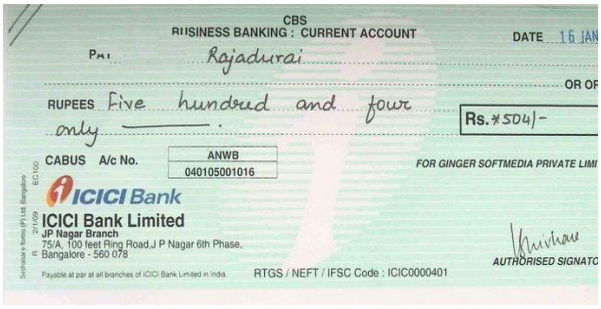


Fig.4 Original Image

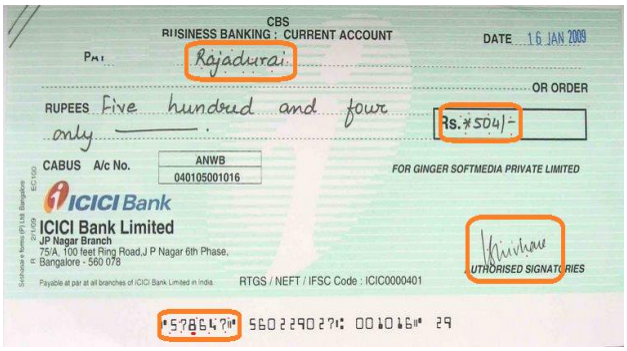


Fig.5 Selected area where digital Watermarking data reside

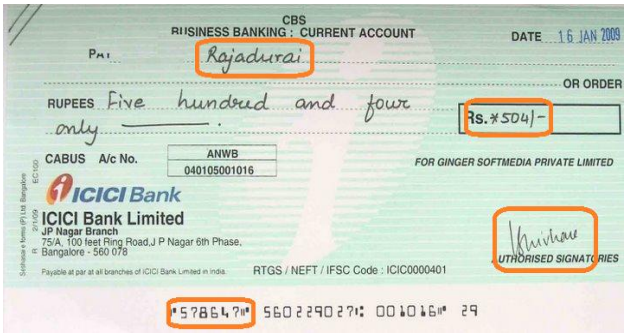
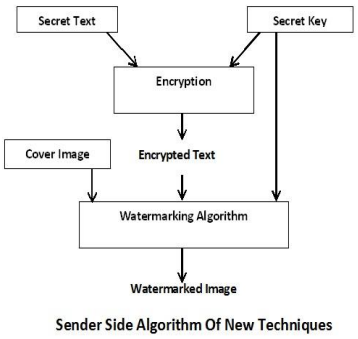


Fig.6 Watermarked Image

Embedding process

The embedding process involves selecting sensitive part of image with the help of rectangle, calculating characteristic values from the pixels and hiding data process. More details will be discussed in the following subsections:



Sender Side Algorithm Of New Techniques

Fig.7 Embedding process

Algorithm 1 Text Encryption

Input : P_t ,Key

Output : Kt

KEY=Concate(key,key,key,key,key,key,key,key)
Choose first eight characters from KEY as (k1,k2,k3,k4,k5,k6,k7,k8)
Finalkey=ascii(k1)+ ascii(k2)+ ascii(k3)+ ascii(k4)+ ascii(k5)+ ascii(k6)+ascii(k7)+ ascii(k8)

N3=FinalkeyMOD10
N2=(Finalkey / 10) MOD 10

N1 =(Finalkey/100) MOD 10

For r = 1 to R do // R length of Plain Text (P_t)

If (r mod 3 = 0)

K_t [r]=char(ascii(P_t [r])+N1)

If (r mod 3 = 1)

K_t [r]=char(ascii(P_t [r])+N2)

If (r mod 3 = 2)

K_t [r]=char(ascii(P_t [r])+N3)

End for

Return K_t

Algorithm 2 Watermark Encoding

Input: *D, w, S_T, S_L, S_B, S_R*
// D Original Image, W watermark text in binary, *S_T, S_L, S_B, S_R are Sensitive area top,left,bottom and right positions*
Output:*D_w // D_w Watermarked image as output*

$X=S_L$

$Y=S_T$

$D_W=D$

For i=1 to n do
//loop will iterate for all watermark bits w from 1 to length n of the watermark

$D_W(X,Y).lsb=W_i$

X=X+1 ;

If ($X > S_R$)

$X=S_L$

Y=Y+1

end if

end for

return $D_{w,}$n

Extraction Process:

The original image and data will retrieve by the reverse process.

I. Get the watermarked-image

II. Choose the rectangle pixels

III. Get the secret data

Algorithm 3 Text Decryption

Input : K_t ,Key

Output : Pt

KEY=Concate(key,key,key,key,key,key,key,key)
Choose first eight characters from KEY as (k1,k2,k3,k4,k5,k6,k7,k8)
Finalkey=ascii(k1)+ ascii(k2)+ ascii(k3)+ ascii(k4)+ ascii(k5)+ ascii(k6)+ascii(k7)+ ascii(k8)

N3=FinalkeyMOD10
N2=(Finalkey / 10) MOD 10

N1 =(Finalkey/100) MOD 10

For r = 1 to R do // R length of Cypher Text (K_t)

If (r mod 3 = 0)

P_t [r]=char(ascii(K_t [r])-N1)

If (r mod 3 = 1)

P_t [r]=char(ascii(K_t [r])-N2)

If (r mod 3 = 2)

P_t [r]=char(ascii(K_t [r])-N3)

End for

Return P_t

Algorithm 4 Text Recovery

Input: *D_w,n, S_T, S_L, S_B, S_R*

// D_w Watermarked Image,n watermarked text length, *S_T, S_L, S_B, S_R are Sensitive area top,left,bottom and right positions*
Output: W *// W Watermarked Text*

$X=S_L$

$Y=S_T$

For i=1 to n do
//loop will iterate for all watermark bits w from 1 to length n of the watermark

$W_i =D_W(X,Y).lsb$

X=X+1 ;

If ($X > S_R$)

$X=S_L$

Y=Y+1

end if

for end

return W

IV RESULT

In this section we demonstrate the effectiveness of our proposed methodology. The simulation is done on MATLAB2012a & analysis of our method is performs using PSNR and robustness of image. This method is applied to several images. We use 128 Bytes plain text and 512X512 image in our experiment. We can embed 128 bytes in the original image with the help of robust and reversible watermarking which is shown in Figure 4. The watermarked image is shown in Figure 6. At the receiver end we successfully extract the data without any data loss.

PSNR: It is the ratio between the maximum probable power of a signal and the power of corrupting noise that influences the fidelity of its representation. For the reason that many signals have a extremely extensive dynamic range, PSNR is typically expressed in terms of the logarithmic decibel scale.

The PSNR (in dB) is defined as

$$PSNR = 10log_{10}\frac{MAX_I^2}{MSE}$$

Table I
RESULTS SHOWN FOR 512X512X24 COLOR IMAGES

	Color Image
PSNR(dB)	34.1
Robustness	1.5

Note that there is no noise in all of tests since the proposed and the embedding capacity can range from 512 to 1024 bits for the purpose of authentication, and according to the applications it can be adjust by changing the block size. As shown later the PSNR is much higher than that obtained by using the method in.

Here we can see that by using reversible watermarking technique in the selected sensible area PSNR value of image does not change so that we have correct data at the receiver side.

V CONCLUSION

. In this paper reversible watermarking technique is used for embed data or message in image. Reversible watermarking techniques are used to cater to such scenarios because they are able to recover original data from watermarked data and ensure data quality to some extent. In addition, embedding the information of the watermark into the watermarked image by a reversible Watermarking method can successfully recover the original image. The image quality of the reversible watermarked image is similar to the watermarked image. Experimental results show that our method can clearly display a watermark and can completely remove the watermark. The future work is to extend proposed technique for videos and to modify given scheme to improve the image quality. The key size and the image size are fully user dependent, So that in future this could be implemented fully independent from user and take automatically image size according to data size.

REFERENCES

[1] Saman Iftikhar, M. Kamran and Zahid Anwar“ RRW - A Robust and Reversible Watermarking Technique for Relational Data”. Published in Knowledge and Data Engineering, IEEE Transactions on (Volume:PP , Issue: 99).

[2] Bajaj, A. “Robust and reversible digital image watermarking technique based on RDWT-DCT-SVD”. Advances in Engineering and Technology Research (ICAETR), 2014 International Conference.

[3] Kavipriya, R. ; Dept. of EEE, Kongu Eng. Coll., Perundurai, India ; Maheswari, S.” Statistical quantity based reversible watermarking for copyright protection of digital images” Published in Green Computing Communication and Electrical Engineering (ICGCCEE), 2014 International Conference.

[4] K. Jawad and A. Khan, “Genetic algorithm and difference expansion based reversible watermarking for relational databases,” Journal of Systems and Software, 2013.

[5] J.-N. Chang and H.-C. Wu, “Reversible fragile database watermarking technology using difference expansion based on svr prediction,” in Computer, Consumer and Control (IS3C), 2012 International Symposium on. IEEE, 2012, pp. 690–693.

[6] M. E. Farfoura, S.-J. Horng, J.-L. Lai, R.-S. Run, R.-J. Chen,and M. K. Khan, “A blind reversible method for watermarking relational databases based on a time-stamping protocol,” Expert Systems with Applications, vol. 39, no. 3, pp. 3185–3196, 2012.

[7] X. Li, B. Yang, and T. Zeng, “Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection,” Image Processing, IEEE Transactions on, vol. 20, no. 12, pp. 3524–3533, 2011. IEEE First AESS European Conference on. IEEE, 2012, pp. 1–6.

[8] E. Sonnleitner, “A robust watermarking approach for large databases,” in Satellite Telecommunications (ESTEL), 2012

[9] M. E. Farfoura and S.-J. Horng, "A novel blind reversible method for watermarking relational databases," in Parallel and Distributed Processing with Applications (ISPA), 2010 International Symposium on. IEEE, 2010, pp. 563–569.

[10] G. Gupta and J. Pieprzyk, "Database relation watermarking resilient against secondary watermarking attacks," in Information Systems Security. Springer, 2009, pp. 222–236

[11] D. M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," Image Processing, IEEE Transactions on, vol. 16, no. 3, pp. 721–730, 2007.

[12] K. Huang, H. Yang, I. King, M. R. Lyu, and L. Chan, "Biased minimax probability machine for medical diagnosis," in Proceedings of the 8th International Symposium on Artificial Intelligence and Mathematics (AIM04), 2004.

[13] D. M. Thodi and J. J. Rodriguez, "Reversible watermarking by prediction-error expansion," in Image Analysis and Interpretation, 2004. 6th IEEE Southwest Symposium on. IEEE, 2004, pp. 21–25.

[14] A. M. Alattar, "Reversible watermark using difference expansion of triplets," in Image Processing, 2003. ICIP 2003. Proceedings. 2003 International Conference on, vol. 1. IEEE, 2003, pp. I–501.

[15] Y. Zhang, B. Yang, and X.-M. Niu, "Reversible watermarking for relational database authentication," Journal of Computers, vol. 17,no. 2, pp. 59–66, 2006.

[16] Î. Chen and G.W. Wornell "Achievable performance of digital watermarking systems", IEEE Int. Conf. on Multimedia Computing & Systems, vol. 1, pp.13 -18 1999.

[17] I. Pitas "A method for watermark casting in digital images", IEEE Trans. on Circuits and Systems on Video Technology, vol. 8, no. 6, pp.775 -780 1998.

[18] I.J. Cox and P. Linmartz "Public watermarks and resistance to tampering", IEEE Int. Conf. on Image Processing, vol. 3, no. 0_3-0_6, 1997.

[19] M. Costa "Writing on dirty paper", IEEE Trans. on Information Theory, vol. 29, no. 3, pp.439 -441 1983.

[20] Y. Seki, H. Kobayashi, M. Fujiyoshi, and H. Kiya, "Quantization- based image steganography without data hiding position memorization," in Proc. IEEE ISCAS, 2005.

[21] Asikuzzaman, M.; Alam, M.J.; Lambert, A.J.; Pickering, M.R., "A blind watermarking scheme for depth-image-based rendered 3D video using the dual-tree complex wavelet transform," Image Processing (ICIP), 2014 IEEE International Conference on , vol., no., pp.5497,5501, 27-30 Oct. 2014.

[22] Kuroda, H.; Imamura, K.; Fujimura, M., "Search Method Using the Pixel Value Histogram of ROI for Illegal Copy Image with Geometric Attacks," u- and e- Service, Science and Technology (UNESST), 2014 7th International Conference on , vol., no., pp.3,6, 20-23 Dec. 2014.

[23] Fujiyoshi, M., "A near-lossless data hiding method with an improved quantizer," Circuits and Systems (ISCAS), 2014 IEEE International Symposium on , vol., no., pp.2289,2292, 1-5 June 2014.

