SCIENTIFIC RESEARCH CENTER
International Journal of Research in Science and Engineering ,ISSN: **2347-9353**
Volume 1, Issue 3,July 2016,,PP44-54

THE SURVEY AND IMPROVEMENT OF DIGITAL WATERMARKING BASED ON IMAGE AUTHENTICATION TECHNIQUES

Akbar Alamian

M.A in Electronic Engineering, Azad University, Yazd Branch

***Abstract**:*

In this paper, a new method for blind digital image water marking, to improve authentication in this kind of images is proposed. In the first method, the host image is divided into blocks of 8 × 8, then turn Ridgelet taken from each block. This procedure is used by the algorithm roposed in this ch. The simulations clarity, strength, and capacity of the proposed method in comparison with other similar are shown. Jpeg compression efficiency of the proposed method for processing such as Gaussian noise and resistance are welcome.

***Keywords**: authenticity verification, Ridgelet conversion, watermarking*

Introduction:

Authenticity verification problem can be described as follows:

Digital message M the sender S to the receiver R sends the message by R must be check following three conditions:

This is exactly the message that is sent by the transmitter S au-century (check accuracy)

(B) The sender actually sent by the sender S (check accuracy)

(C) The sender S cannot claim that the message M is sent (non-repudiation)

In ancient Greece watermarking is used only to communicate secretly. Tales of tablets that were written with invisible oils or slaves were tattooed with the message or the messenger scalps taken on the messages devoured, suggests that in the distant past have often been used by humans as hosts. Today, instead of a man of multimedia products for the home signal is used and watermarking of digital watermarking has become [1, 2].

Steganography is a process during which the data in other formats, such as image files or text shapes and hide. Your journalism is a branch of science called hidden secret communication. Knowledge of communications covered includes several branches including encryption, the encryption and much more. The main objective of the digital watermarking, information embedding image watermarking is invisible and robust form of digital content. The most popular method of hiding data in files is the use of graphic images as hiding places. The image is supposed to be an information carrier is the carrier image and the input image or data that can result is called the latent image. Watermarking is a message encoded in the original signal (host) embedded only by knowing the secret key can be extracted from the original message. Watermarking is one of the ways to implement the information hiding is presented. By placing watermarking information such as a company logo and licensing, intellectual

property rights to protect the home and goes to work. The simplest method that was introduced in the first place the data in the least significant bit of the pixel intensity image. It was also easy to use with very little time is needed and the volume of data is too large to hide. For example, in an image with dimensions of 256 × 256 pixels, 8 kilobytes of data can be stored this way. This method is highly visible in the image but its main problem is which create the slightest change in the image, all data will be destroyed and it does not secure the data [2, 3].After that like shade technique [4], statistical methods [5, 6], range [7, 1], Fractal [8] as well as methods based on Cosine [9], Fourier [10] and Wavelets [11] has been proposed. Today, scientists are researching methods based on human visual system to maintain image quality while watermarking, the time required to extract data and also extract data without the original image are [2, 12]. Each method has a number of strengths and weaknesses of steganography is evaluated based on three criteria listed (capacity, stability and security) are evaluated. In this study, the DCT steganography method based authentication will do. This method is a method based on Fourier transform.

SCIENTIFIC RESEARCH CENTER
International Journal of Research in Science and Engineering ,ISSN: **2347-9353**
Volume 1, Issue 3,July 2016,,PP44-54

The proposed method

The proposed watermarking algorithm is an algorithm based on the Inoyeh. This algorithm is a string of binary image watermarking hides. To convert an image watermarking Rejlat taken up and the band splits n Hn is selected for watermarking. For the conversion of Fyatr Dabychz is used. Assuming that W is a bit string of length K, which is supposed to be hidden in the image P and the dimension bfx * bfx block Bk is converted from Hn and MK mean is that each of these blocks of Bk if the quantization factor and Qf according to equation (1) is determined by the relationship m is a natural constant, put the following steps in the process of watermarking is done:

Equation (1) Qf = m * 2n

The first step of the ridgelet transform the image to be taken of the decomposition of n and Hn the conversion coefficients for adding data selection. It is chosen because the area is the lack of sensitivity of the human eye to changes at high frequencies.

The second step: selection of the smaller block Bk split bfx * bfx dimensions, the block scheme in Figure 1 is shown.

Figure 1: The block Hn and select the row of the block

Step Three: Average block Bk is quantized so that if W (K) is zero, and if the even value $\left[\frac{Q_k}{Qf}\right]$ is the amount is odd $\left[\frac{Q_k}{Qf}\right]$.

Step Four: After placing the image image image watermarking has become Ridgelet taken and will be ready for distribution.

The category Hn block in Figure 1 is shown.

The larger the size of Bk is more resistant watermarking in image processing, but the amount of data that can be hidden in the image is reduced so as to choose the appropriate size for the Bk to be compromised.

Watermarking extraction process

Must be extracted in the following steps:

Step One: The converted image Ridgelet taken and assigned to the decomposition of n subband desired, data can be extracted.

Step Two: Insert the block selection, as the smaller the dimensions bfx * bfx Bk split.

Step Three: If the average block Bk is calculated as zero-bit watermarking $\left[\frac{Q_k}{Qf}\right]$ even if the person is mined and extracted value.

DISCUSSION

CCITT is used to test three binary images. Each image dimensions of 512 x 512 pixels which are stored in TIFF format and no compression has been done on them. Length of 128 bits is stored. All experiments are based on the level of decomposition Dabychz filter 3, 2 and 1 have been carried out by a factor of 2 or 4.

Effect of number of decomposition levels Ridgelet become the watermarking

For this test, the criteria to be considered invisible, and PSNR, the PSNR of the equation (2) is calculated:

Equation (2)

$$PSNR = 10log10\left(\frac{255^2}{mse^2}\right)dB$$

Mse2 mean-square difference between the brightness of the original image is the image watermarking. Experimental results show that PSNR for a specific image by changing n does not cause errors. In Figure 2 graphs changes in the extraction of 128-bit errors in image

SCIENTIFIC RESEARCH CENTER
International Journal of Research in Science and Engineering ,ISSN: **2347-9353**
Volume 1, Issue 3,July 2016,,PP44-54

watermarking based on changes m CCITT2 show. As can be seen, in the graph watermarking strength increased with increasing m.

Figure 2: PSNR graph for image CCITT2 by changes m the determinant of Qf is

The effect of JPEG compression

Compressed images in Figure 3 is also shown in Figure 4 is the variation of the error terms qf changes. As can be seen in Fig so that the image can be used for good compression rate is low error rate is maximum error rate in compression by a factor of 2 is the quantity should be these factors decrease the quantity of picture that is easily visible by the human eye the quality factor of 80, 90 and 95 are conventional compression rates are the margin of error is less than 5 percent, the proposed method of resistance against this attack is acceptable.

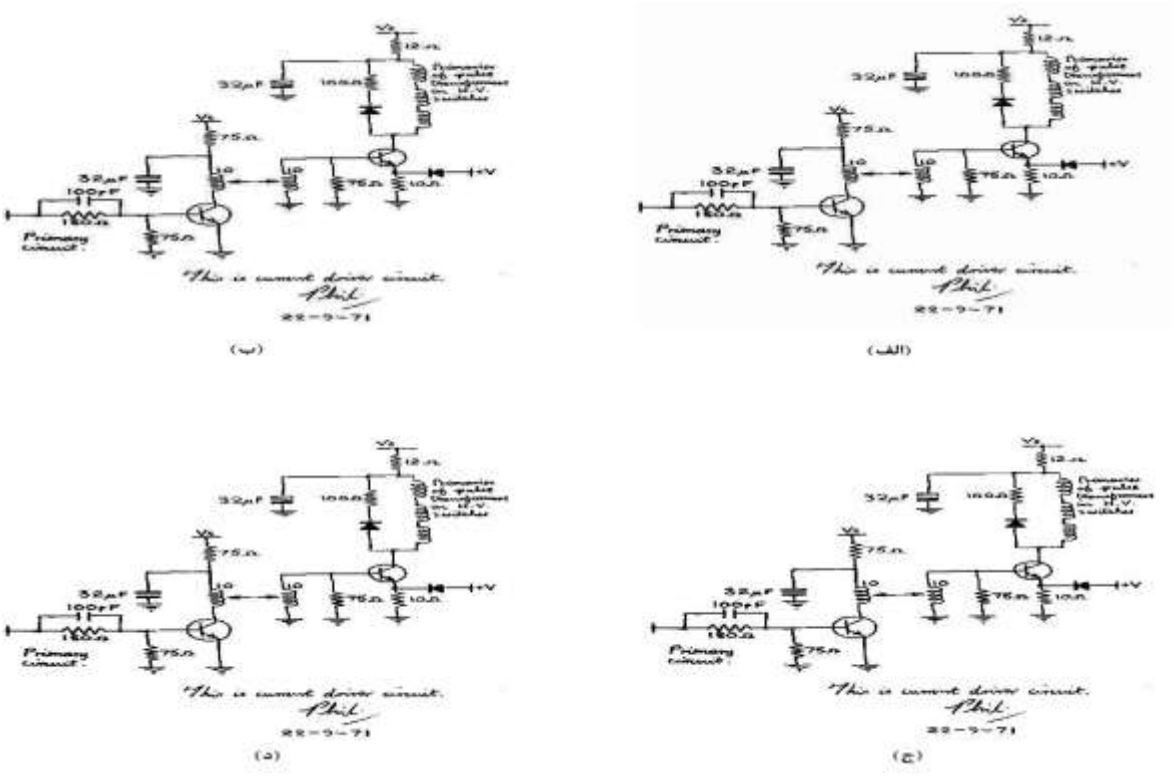

Figure 3: images compressed with different quality factors, (a) the factor 20, (b) the factor 10, (c) a factor of 90, and (d) a factor of 95.

SCIENTIFIC RESEARCH CENTER
International Journal of Research in Science and Engineering ,ISSN: **2347-9353**
Volume 1, Issue 3,July 2016,,PP44-54

As can be seen in the compressed image quality is still good, the error is less than 10%. Most errors in the graph compression with quality factor of 10%, which is roughly equivalent 0.25 rate compression, image distortion will be obvious in this case.

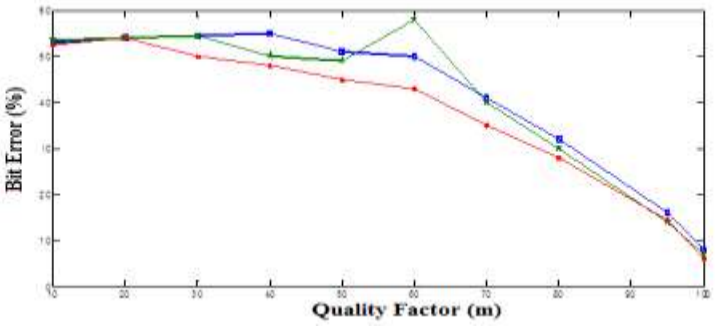

Figure 4: Graph of error changes in QF

The effect of adding Gaussian noise

In this experiment, the image watermarking Gaussian noise with mean zero and standard deviation of G increases. Figure 5 Diagram of the reconstruction error against the noise changes.

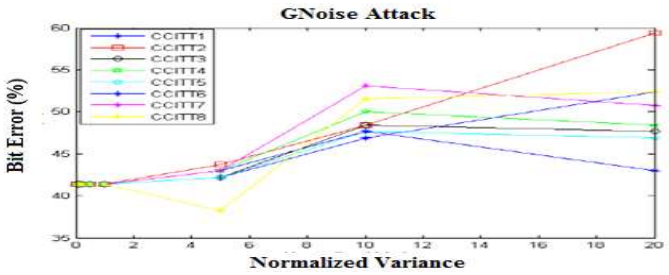

Figure 5: Graph of error changes depending on the variance of the Gaussian noise

SCIENTIFIC RESEARCH CENTER
International Journal of Research in Science and Engineering ,ISSN: **2347-9353**
Volume 1, Issue 3,July 2016,,PP44-54

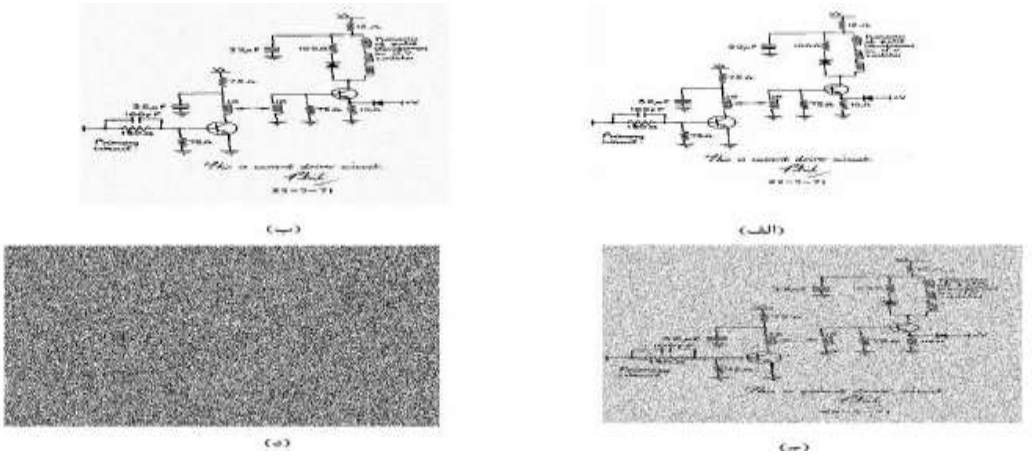

Figure 6: Image watermarking with the Gaussian noise variance of the variance for (a) 0.02, (b) 0.1, (c) 0.5 and (d) 2.

In Figure (7) graph in terms of the reconstruction error variance Gaussian noise (normalized variance, shows the variance of 42 is normally 0.1).

According to the graph, the maximum margin of error greater than 2 is the noise variance the noise effect on the image's quite clear that the image cannot be used. The noise variance is low, the error is less than 0.5, and the image reconstruction is an acceptable level is less than 45 percent. The impact of these attacks to various images almost the same results.

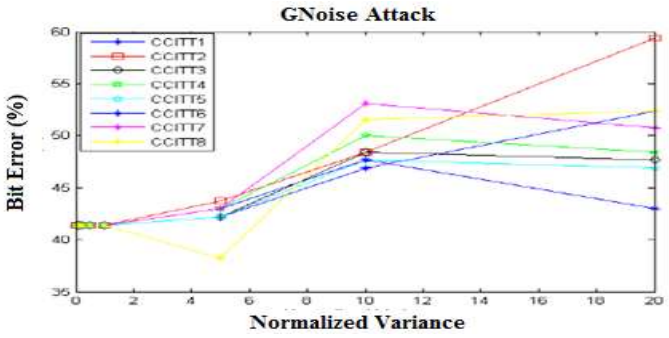

Figure 4_ 15: Graph of error changes depending on the variance of the Gaussian noise

Table 1 shows the overall results after 230 iterations and extracting watermarking attacks And the mean extraction hundred percent correct answers can be answered based on the RT algorithm is much better.

Table 4_ 1: Comparison of proposed method and algorithm base

name of the algorithm	proposed algorithm	basic algorithm
Frequency of occurrence of attacks	230	230
number of successful detection	218	190
Percentage of successful detection	94%	82%

References

- L.M.Marvel , "Image steganography for hidden communication",PHD thesis,University of Delware,spring 1999
- L.M.Marvel et al., "Spread spectrum image steganography",IEEE Transactions on Image Processing.Vol.8,No.8,pp.1075-1083,Aug 1999.
- W.Zhu et al.,"Multiresolution watermarking for Images ond video",IEEE Transactions on Circuits and Systems for Video Technology,Vol.9,No.4,pp.545-550,June 1999.
- . Rare Samsvnchy approach to digital watermarking of images, MS Thesis, Tarbiat Modarres University, 1999.
- W.Bender et al.,"Techniques for datahiding",IBM systems journal,Vol.34,Nos.3&4,pp.313-316.
- W.Bender and D.Gruhl.,"Information Hiding to Foil the Casual Counterfeiter ",Second International Information Hiding Workshop,Lecture Notes in Computer Science,pp.1-15,April 1998.
- J.J. Cox et al.," Secure spread spectrum watermarking for multimedia",IEEE Transactions on Image Processing,Vol.6,No.12,pp.1673-1687,Dec.1997.

- P.Bas et al.,"Using the fractal code to watermark images",Proceedings of the IEEE Inter.Conf.on Image Processing,Vol.I,pp.469-473,1998.
- C.F.Wu,W.S.Hsieh,"Digital watermarking using zerotree of DCT ", IEEE Transactions on Consumer Electronics.Vol.46,No.1,,pp.87-94,Feb.2000.
- S.Pereira and T.Pun,"An iterative template matching algorithm using the Chirp-Z transform for digital image watermarking ",Pattern Recognition,Vol.33,No.1,pp.173-175,Jan.2000.
- M.Ejima and A.Miyazaki,"A wavelet based watermarking for digital images and video",IEICE Transactions on Fundamentals of Electronics,Communications and computer Science,Vol.E83 A,No.3,pp.532-540,March 2000.
- M.J.Tsai et al.,"Joint wavelet and spatial transformation for digital watermarking", IEEE Transactions on Consumer Electronics,Vol.46,No.1,pp.237,Feb.2000.