ISSN: 2321-7782 (Online)
Impact Factor: 6.047

Volume 5, Issue 1, January 2017

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Comparative Analysis of Arnold-Chaos and Arnold Chaos-RSA Techniques Based Blind Digital Image Watermarking

Shubhangi Pande[1]
M.Tech, IV Semester
Department. Of CSE
LNCT, Indore (M.P.) – India

Santosh Varshney[2]
Associate Professor
Department. Of CSE
LNCT, Indore (M.P.) – India

Abstract: The digital watermarking method embeds meaningful information into one or more watermark images hidden in one image, in which it is known as a secret carrier technique. It is difficult for a hacker to extract or remove any hidden watermark from an image, and especially to crack so called digital watermark technique. In this paper, a hybrid blind digital watermarking algorithm is presented which is robust enough to resist the watermark against the attacks. The algorithm exploits the random sequence generated by RSA, Arnold and Chaos transformations. Discrete wavelet transformation of second level decomposition is used to convert the image into its frequency domain. Simulation result shows the performance of watermarking of image against attacks. In the end, the performance of the proposed technique will be measured on the basis of PSNR, and NCC and MAE.

Keywords: Embedded, Watermarking, Image, DWT, DCT, Arnold transform, Chaos transform, RSA, Frequency domain Robust, Blind, etc.

I. Introduction

In the recent times, the growth of internet is so vast that it is penetrating in the remote areas even where the person need hard work to reach such areas, the internet is available there also shows the growth of penetration in the world, the data can be easily transferred to the other person in just a single click, with the reducing time for outdoor entertainment. Due to busy lifestyle, the only source of entertainment is television or computers. Then, if someone is getting the entertainment on computer just like television then it will be great option for everyone. The digital representation of media files possesses advantages of portability, efficiency and accuracy of information content. This is the reason that piracy is in full swing. Everybody wants latest images, audio files or video files and they are getting it on the internet, and free of cost. For the original producer of the file even doesn't know that the file created by him/her is available for free by internet and even if know. Here is the point, when the need of some method comes in so that the actual producer can prove that the file belongs to him/her.

Digital watermarking techniques is the process that embeds data, called aa watermark system, into a multimedia object in such a manner that the watermark scheme can be detected or extracted later to make a decision about the copyright of the object. The digital watermarking technique, a specific code or mark is embedded permanently inside a cover multimedia file which remains within that cover invisibly or visibly even after decryption process [1-2].

In this paper, a wavelet based watermarking technique is used by using RSA, Arnold and chaos transform.

II. Related Work

The many researchers have been done significant work in the field of watermarking techniques Based different wavelet transform problem, some of the work is described in this:

Zheng-Wei Shen, in this paper, wavelet and Henon chaos for the encryption of watermark. Chaos transform has irregular movement which looks like random and occurs in a deterministic system. Although chaos is a deterministic describing system, its behavior is uncertain. The method is invisible and robust against some usual attacks such as JPEG, cropping, adding noise and filtering [1].

Mohamed A. Mohamed, in this paper the proposed combination of the two transforms improved the watermarking process performance considerably when compared to single watermarking techniques. In general, combining more than one digital watermarking technique; especially in transformed domain, highly improves both robustness and capacity of watermarking [2].

Qiang Wang, during the embedding of the watermarking, discrete wavelet transform is done firstly and extracted the low frequency part as the embedding field; the chaotic sequence was used to encrypt the watermark and transform the encrypted part and extract the low frequency; finally, authors embedded the low frequency part into that of the original image. Authors extracted the watermark non-blindly [3].

Reena Anju, The described an imperceptible and a robust combined discrete wavelet transform discrete cosine transform digital image watermarking algorithm. The algorithm watermarked a given digital image using a combination of the Discrete Wavelet Transform and the Discrete Cosine Transform (DWT-DCT). Performance evaluation results show that combining the two transforms improved the performance of the watermarking algorithms that are based solely on the Discrete Wavelet Transform [4].

III. PROPOSED METHOD

The proposed method is made up after concluding the literature survey. It utilizes the advantages of wavelet transform, RSA method, Arnold Transform and Chaos transform. Two encryption techniques are used to enhance the security of the watermark.

1. ARNOLD METHOD

The Arnold transform is a classical 2D invertible chaotic map defined as:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \left[\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \ (mod\ 1) \right] \qquad (1)$$

Arnold transformation defined by (1) is a one-to-one transformation. From the view of sampling theory, digital images can be viewed as a matrix of 2D discrete points derived from sampling according to a certain interval and a certain method. Square matrix of digital images can be made discrete by Arnold transformation.

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \left[\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \ (mod\ N) \right] \ (x, y) \in 0,1,,2 \dots \dots \dots .., N-1 \qquad (2)$$

Equation (2) is used to transform each and every pixel coordinates of the images. When all the coordinates are transformed, the image we obtain is scrambled images. In addition, when one digital image is transformed by Arnold transformation, the transforming process can be achieved continually. At a certain step of iteration, if the image we achieve reaches our anticipated target, we have achieved the scrambled image we need. The decryption of image relies on the transformation periods. The periods change in correspondence to the size of images. The iteration periods is 96 for a 128×128 image; 48 for a 64×64 image. Here the number that images are scrambled is used as an encryption key and modulated by binary pseudo random sequence, which further strengthens the security of watermark.

2. RIVEST-SHAMIR-ADLEMAN

The RSA cryptosystem, named after its inventors R. Rivets', A. Shamir, and L. Adelman, is the most widely used public key Cryptosystem. It may be used to provide both secrecy and digital signatures and its security is based on the intractability of the integer factorization. The RSA algorithm involves three steps: key generation, encryption and decryption.

a) **Key generation**

RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated the following way:

To generate the two keys, choose two random large prime numbers p and q. For maximum security, choose p and q of equal length. Compute the product

$$K = P * Q$$

Then randomly choose the encryption key e such that e and (p −1) (q −1) are relatively prime. Finally, use the extended Euclidean algorithm to compute the decryption key d such that

$$d = e^{-1} mod((p-1)*(q-1)) \quad (3)$$

b) Encryption

Firstly receiver transmits her public key (n, e) to sender and keeps the private key secret. If sender wishes to send message M to receiver. Sender change the message M in to integer m, such that 0 ≤ m

$$C = m^{e}(mod\, n) \qquad (4)$$

c) Decryption

Receiver can recover m from c by using her private key exponent d via computing

$$M = c^{d}(mod\, n) \qquad (5)$$

3. CHAOTIC ENCRYPTION

Chaos signals are a kind of pseudorandom, irreversible and dynamical signals, which process good characteristics of pseudorandom sequences. Chaotic systems are highly sensitive to initial parameters. The output sequence has good randomness, correlation, complexity and is similar to white noise. Chaotic sequence has high linear complexity and non-predictability. The model [11] here is chaos 1-D Logistic and is shown.

$$x(n+1) = \mu * x(n) * [1 - x(n)] \quad (6)$$

Where μ (0, 4); x (n) (0, 1). By initializing μ and x (0), we can get the required chaotic signal. In order to get chaotic sequences, the chaotic signal x (n) must be transformed into binary sequence s (n). So quantized function T[x (n)] is used and can be given by (4).

$$T[x(n)] = \begin{cases} 0 & x(n) \in U_{k=0}^{2^{m-1}} \quad I_{2k}^{m} \\ 1 & x(n) \in U_{k=0}^{2^{m-1}} \quad I_{2k=0}^{m} \end{cases} \qquad (7)$$

Where m is random integer and should be greater than 0. (I_0^m,…….).is continuous equal interval in [0, 1] and the interval is divided by 2^m . If the value is in the odd interval of the quantized function, the quantized value is 1, or else, the quantized value is 0. The binary sequences generated were of good pseudorandom sequence characteristics. Chaotic key sequence are XORed by binary image, generated the encrypted watermark image.

IV. Experimental Results

The proposed idea is implemented in MATLAB software which is extensively used in all regions of applied mathematics. The proposed method is the hybrid technique which involve Arnold Transform, RSA and Chaos Transform, which improve the security of digital images at very much extent compared to existing one. Here, we are using the concept of gain factor in coding, which result that it increases the PSNR (Peak signal to Noise Ratio) value. Increment in the PSNR value also means that embedding is very much strong and chances of attack is low. The other two performance parameters on the basis of experimental results are evaluated are: MAE (Mean Absolute Error) and NCC (Normalized Cross Correlation). MAE gives the difference between an original watermark and extracted watermark. Robustness of system is measured by lower the value of MAE. In opposite, larger the value of NCC, similarity between images are more. NCC range is [0, 1].

Images	*PSNR*		
	Previous Algo.	*Proposed Algo.*	
		G.F- 0.1	*G.F- 0.5*
Lena_gray	51.1402	74.1514	60.1720
Cameraman	51.1423	74.1514	60.1720
Mandrill_gray	51.1403	74.1514	60.1720
Lena_color	51.1401	74.1514	60.1720
Mandrill_color	51.1403	74.1514	60.1720

Table 1:- Experimental results of comparison between existing and proposed algorithm (without attack)

Above table shows that our proposed algorithm is very much strong as compared to previous algorithm, as its PSNR value is high during embedding. Also, at the particular gain factor value, its PSNR value is constant for any type of square image.

Table 2, Table 3, Table 4, Table 5, Table 6 gives the information of MAE and NCC value during extraction of watermark in case of various attacks such as Salt & Pepper noise (density-0.02), Speckle noise (density-0.02), Gaussian noise, Median Filer and Poisson noise respectively.

Attack	*Images*	*MAE*		*NCC*	
		Previous algo.	**Proposed algo.**	**Previous algo.**	**Proposed algo.**
Salt & Pepper Noise (0.02)	Cameraman	0.0392	0.0337	0.9023	0.9154
	Lena_color	0.0369	0.0353	0.9245	0.9275
	Mandrill_color	0.0390	0.0380	0.9220	0.9239

Table 2: Extracted watermark in case of Salt & Pepper noise.

Attack	*Images*	*MAE*		*NCC*	
		Previous algo.	**Proposed algo.**	**Previous algo.**	**Proposed algo.**
Speckle Noise (0.02)	Cameraman	0.4436	0.0644	0.0967	0.8422
	Lena_color	0.4760	0.0582	0.0475	0.8809
	Mandrill_color	0.4722	0.0519	0.0555	0.8961

Table 3: Extracted watermark in case of Speckle noise.

Attack	*Images*	*MAE*		*NCC*	
		Previous algo.	**Proposed algo.**	**Previous algo.**	**Proposed algo.**
Gaussian Noise	Cameraman	0.2685	0	0.4174	1
	Lena_color	0.2694	0	0.4560	1
	Mandrill_color	0.2696	0	0.4607	1

Table 4: Extracted watermark in case of Gaussian noise.

Attack	*Images*	*MAE*		*NCC*	
		Previous algo.	**Proposed algo.**	**Previous algo.**	**Proposed algo.**
Median Filter	Cameraman	0.4551	0.3173	0.0803	0.3276
	Lena_color	0.4837	0.3333	0.0325	0.3297
	Mandrill_color	0.4980	0.4039	0.0039	0.1921

Table 5: Extracted watermark in case of Median Filter.

Attack	*Images*	*MAE*		*NCC*	
		Previous algo.	**Proposed algo.**	**Previous algo.**	**Proposed algo.**
Poisson Noise (0.02)	Cameraman	0.4502	0.0063	0.0873	0.9838
	Lena_color	0.4622	0.0054	0.0741	0.9889
	Mandrill_color	0.4624	0.0044	0.0752	0.9911

Table 6: Extracted watermark in case of Poisson noise.

From the above results, we shows that our proposed watermarking technique is very much strong as compared to previous one in case of attack also.

V. Conclusion

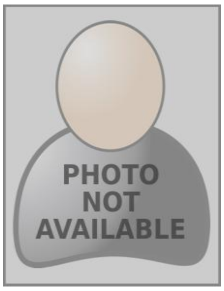
We have implemented a hybrid technique based blind digital image watermarking which involve Arnold transform, Chaos Transform and RSA. It consist of transformation in the image & then the image is totally diffracted, so nobody could see that what information could be shown through that image. With cryptography, image is doubly protected. In the future, we can extend this concept for audio and videos also and can use other cryptographic technique which consume less processing time.

References

1. Zheng-Wei Shen, Ya-Nan Shen, “Blind Watermarking Algorithm Based On Henon Chaos System And Lifting Scheme Wavelet”, International Conference on Wavelet Analysis and Pattern Recognition, 12-15 July 2009.
2. Mohamed A. Mohamed, Abou-Soud, Mai S. Diab, “Fast Digital Watermarking Techniques for Still Images”, International Conference on Networking and Media Convergence, Cairo, Egypt, 2009.
3. Qiang Wang, Zhong Zhang, Lina Ding, “Digital Image Encryption Research Based on DWT and Chaos”, Fourth International Conference on Natural Computation, 2008.
4. Reena Anju and Vandana, “Modified Algorithm for Digital Image Watermarking Using Combined DCT and DWT”, International Journal of Information and Computation Technology, Volume 3, Number 7, 2013.
5. Shashank M Rao, Srujan R, Madhukar V, H S Rahul, Sandeep K V, “ A Secure Color Image Watermarking Scheme Using RSA Encryption”, IJESC, Volume 6 Issue No. 5, 2016.
6. J.L. Liu, D.C. Lou, M.C. Chang, H.K. Tso, “A Robust Watermarking Scheme Using Self-Reference Image”, Computer standards and interfaces, vol. 28, issue 3, Jan 2006.

Author(s) Profile

Shubhangi Pamde, received the BE degree in Computer Engineering from Mandsaur Institute of Technology, Mandsaur in 2007 and Presently she is pursuing M.tech in Computer Engineering from LNCT, Indore (MP), India



Santosh Varshney, received the BE and M.tech degree in Computer Engineering Govt. engineering college, Bhopal and ICSEI, DAVV in 1993 and 1996 respectively. Presently he is working as an Assistant Professor in CS/IT dept. at LNCT, Indore (MP), India.