ISSN No: - 2456- 2165

A Bi-Level Secured Image Watermarking Using Chaotic Mapping and Multi-resolutional Wavelet Transform

Rahul Gupta
Deptt. of Electronics & Comm. Engg
Yagyavalkya Institute Of Technology
YIT Lane, Sitapura, Jaipur, Rajasthan 302022
rahulgupta.rhlgpt@gmail.com

Anila Dhingra
Deptt. of Electronics & Comm. Engg
Yagyavalkya Institute Of Technology
YIT Lane, Sitapura, Jaipur, Rajasthan 302022
anilayit@gmail.com

***Abstract*— With the broad progress of the internet and the traits in digital verbal exchange and compression technology, digital multimedia contents, similar to track, video and snapshot, can also be disbursed right away across the web to end-users. Many media organizations sell their digital contents now not most effective using CDs and DVDs but also over the internet networks. Probably the most talents issues on dealing with the digital knowledge are that it may be quite simply altered and duplicated without shedding its great. Consequently, without safety and management of digital rights, the digital content material will also be copied and allotted to a huge quantity of recipients, which would cause income loss to media companies. Hence, mental property defense is an urgent hindrance for content owners who're selling and exhibiting digital contents using the web. This articles discuss a robust approach for Image watermarking using Chaotic Mapping and Multi-Resolutional Wavelet Transform. The advantage of using two level hiding is targeted to achieve a promisable accuracy accounted PSNR and NC parameters respectively.**

I. INTRODUCTION

The first technological aspect that content homeowners turn to is cryptography. Cryptography is, as a rule, the most original procedure of shielding digital contents (Cox et al., 2002). The content material is encrypted previous to delivery and a decryption key's supplied best individuals who have bought legit copies of the digital content material. After the receiver has got and decrypted the data, nonetheless, the info is same to the original digital content data and the content material has no additional protection. It is possible for a pirate to purchase the content material, use the decryption key to obtain an unprotected copy of the content material, after which proceed to distribute unlawful copies. For that reason, there is a robust want for a substitute technology that may safeguard digital multimedia content even after it is decrypted. Among the many various technologies, digital watermarking science has the competencies to meet this need[1].

Digital watermarking is a rising science that embeds hidden copyright knowledge straight into the digital multimedia content in one of this manner that it normally remains present. The embedded understanding data is referred to as "watermark."[4]. Ideally, there should be no perceptible change between the watermarked and usual knowledge, and the watermark should be conveniently extractable, trustworthy and powerful in opposition to decryption, re-encryption, compression and long-established signal processing. The information carried using the watermark may also be accessed using a detection algorithm with the support of a secret key and can be used to identify the copyright holder and ensure the right cost of royalties.

It is clear that digital watermarking and encryption technologies are complementing each and every different. For that reason, a reliable digital rights management (DRM) process which is a software that protects intellectual property for the duration of digital content commerce relies on both applied sciences (Kundur and Karthik, 2004). The primary functions of digital watermarking are copyright safeguard, fingerprinting, replica security broadcast monitoring and data authentication. Other applications comprise indexing of movies, medical safeguard and knowledge hiding (Langelaar et al., 2000) [8].

This article concentrates on designing watermarking algorithms making use of chaotic mapping and multiwavelet grow. In case just consider that it possesses framework which had been proven to be useful in picture processing purposes; for instance, the DGHM multiwavelets concurrently possess orthogonality, compact aid, an approximation order of two and symmetry (Geronimo et al., 1994). Thus, multiwavelet-based watermarking for copyright security of digital photo can be probably mentioned. However, the final notion offered right here can be relevant to other types of digital multimedia contents[7].

II. LITERATURE SURVEY

Digital photograph watermarking is likely one of the most standard strategies viewed as software for providing the copyright security of digital pictures. This procedure is based on the direct embedding of extra information into the digital photos. Theoretically, there must be no perceptible difference between the watermarked snapshot and the conventional one. Also, the watermark should be quite simply extractable, however, riskless and potent towards photo compression or original snapshot processing. Through extracting the embedding knowledge, the photograph ownership will also be tested or even an unlawful reproduction supply can be traced[9].

In this chapter, literature surveys of updated digital snapshot watermarking methods discovered in some textbooks and study papers are awarded. Although a huge number of digital photograph watermarking algorithms had been

ISSN No: - 2456- 2165

increasingly launched, many of them are personal watermarking schemes as a result of the need for a customary image in a detection segment. Consequently, the development of a brand new public watermarking scheme which satisfies each invisibility and robustness challenges study aspiration of most researchers in the discipline of digital snapshot watermarking within the 21st century[10].

Spatial domain watermarking methods (Langelaar et al., 2000; Lumini and Maio, 2000)[6] are simple to put into effect and require less computation price than the opposite does. To embed a watermark right into an accurate snapshot is without the doubt straight ahead. A pseudorandom noise sample is generated and then introduced to the luminance price of its pixels centered on key utilizing linear shift registers or randomly shuffled binary portraits (Tirkel et al., 1993).

A discrete cosine turn into (DCT)[7] has been essentially the most ordinarily used transformation system in photo watermarking. One of the vital mentioned watermarking schemes of this technique is proposed employing Cox et al. (1997). The proposed process is performed via embedding a offered watermark into one of the absolute best magnitude discrete cosine transform coefficients (perceptually colossal coefficients) of an image making use of an inspiration of unfolding spectrum verbal exchange. This motivation is founded on the fact that any try and alter the watermark outcome in noticeable degradation of the watermarked image. Considering that the watermark is forged into essentially the most perceptually large regions of the usual snapshot, it is competent to withstand original signal processing and geometric distortions. Nonetheless, this method should not be compatible with many purposes considering that of excessive complexity of global DCT and the necessity for the common picture throughout watermark extraction[9].

Barni et al. (1998)[4] reward a public watermarking algorithm headquartered on Cox's algorithm, but it does not want the traditional image for extracting the watermark. In 1999, block DCT was utilized before embedding the watermark and the watermark is embedded most effective in middle-frequency add-ons of the 8×8 DCT blocks.

In the embedding phase, low-frequency components are left untouched to expand invisibility of the watermark (Hsu and Wu, 1999)[2]. The robustness of a watermark can be elevated by way of growing the vigor of the watermark. Increasing the vigor, however, degrades the photograph satisfactory. Accordingly, to find the pleasant alternate-off between the imperceptibility and robustness to signal processing is one of the principal disorders in digital watermarking.

In literature, several ways have been proposed to enhance the robustness of watermarking algorithms. Podilchuck and Zeng (1998)[9] proposed an equivalent scheme to Cox et al. (1997) via using a knowledge of visible human methods (HVS) in the DCT domain. By way of exploiting the masking effects of the HVS, it is possible to hide a watermark with more energy in a photo. Consequently, the embedded watermark is extremely potent. Zeng and Lei (1999) proposed a blind DCT-centered watermarking algorithm for copyright safeguard of a still photograph and video information. The characteristics of HVS are exploited in an adaptive photograph watermarking scheme to achieve an excessive visual quality of the watermarked snapshot and robustness of the watermark.

Dugad et al. (1998)[1] proposed a spread spectrum photo watermarking manner in the discrete wavelet change into the domain. They embed a watermark message with a constant valued weighting factor into perceptually colossal coefficients in excessive frequency subbands so as to maintain invisibility. Nonetheless, it is not strong to usual signal processing. In 2000, the core suggestion of Hsu and Wu (1999) was multiplied to wavelet become. In watermark embedding approach, each decomposed layer of a binary watermark is embedded into a corresponding decomposed layer of a customary photo. Nevertheless, embedding the watermark in high-frequency add-ons makes this manner fail underneath an assault of excessive frequency factor elimination of the photo (Hsu and Wu, 2000).

Yang (2003)[3] has targeted the evaluation of biorthogonal wavelets using spread-spectrum watermarking framework. An additional method of photo watermarking is proposed through Wang and Lin (2004). They proposed a wavelet tree quantization for copyright defense watermarking. The wavelet coefficients of the fashioned photo are grouped right into a predefined constitution called supertree. Watermark bits are embedded by quantizing the supertree. The change between quantized and unquantized timber is then used for watermark extraction.

III. CHAOTIC MAPPING

Moreover, in picture encryption applications, quite a lot of researchers have targeted themselves on additionally double random plane encoding manner to enhance the protection of procedure wherein random segment masks (RPM) is utilized twice times. In this direction, RPM is developed with support of random numbers generated by conventional chaotic map. The traditional chaotic map is a specific case of the logistic map which is a non-linear polynomial of 2d levels and is expressed as [4,8]:

$$x_{n+1} = \lambda * x_n * (1 - x_n)$$

Where λ is a system parameter lies between 0 to 4, x_n is map variable lies between 0 to 1, x_0 is the initial condition of the logistic map also called seed value and *n* is the number of iterations. After varying procedure parameter λ in-spite of its seed worth, following behaviors are observed: When λ lies within 0 to 1 then iterative values ultimately dies, which can be sovereign of its seed price. When λ lies within 2 to 3 then iterated values first oscillate round some values after which in the end stabilize on same value. When λ lies inside three and 3.45 (approximately) then iterated values oscillate between two values, which are eternally stylish on λ. When λ lies within 3.45 and 3.56 (approximately) then iterated values oscillate between four values.

IV. MULTI-RESOLUTIONAL WAVELET TRANSFORM

The multiwavelet change into is a brand new proposal within the framework of wavelet transforms however has some principal differences. In designated, whereas a wavelet has a scaling operate and a wavelet perform, multiwavelets have two or more scaling functions and correct wavelet capabilities. Some of the recognized multiwavelets was constructed through Donovan, Geronimo, Hardin, and Massopust (DGHM) (Geronimo et al., 1994). DGHM multiwavelets

ISSN No: - 2456- 2165

simultaneously possess orthogonality, compact support, an approximation order of two and symmetry. Next, we supply a brief overview of the multiwavelet develop into. In addition, considering the multiwavelets have a couple of scaling operate, the dilation equation turns into dilation with matrix coefficients. Accordingly, in functions, one need to associate a given discrete sign to a chain of size − r vectors (the place r is the quantity of scaling features) without losing some detailed properties of the underlying multiwavelet. This sort of approach is referred to as profiteering or multiwavelet initialization. The block diagram of a multiwavelet with prefilter Q(z) and post filter P(z) is shown in figure.1 . H(z) and G(z) are the z become of h(n) and g (n) , respectively.

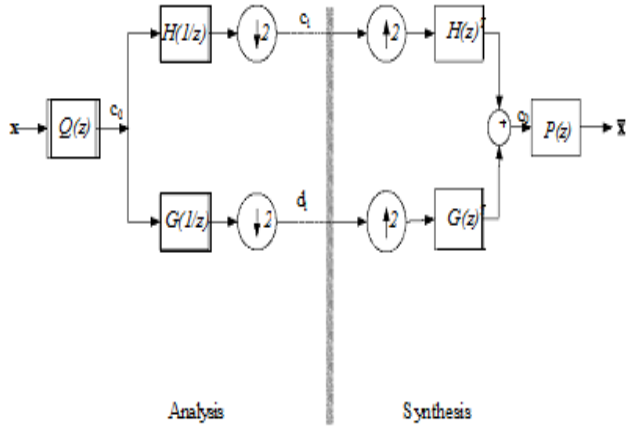


Fig.1. Multi-resolution wavelet decomposition and reconstruction

V. EXPERIMENTAL SETUP & RESULTS

In the proposed art we have tried to exhaust the advantage of chaotic mapping and multi resolutional property of wavelet transform to achieve a robust watermarking scheme for general imaging purposes. The below figure 3 and 4 defines the deployed flow graph for embedding and extraction of message image in the cover image.

The standard images are processed for justifying the results of watermarking. The standard cover and message image set are depicted by fig.2.

Cover Image	Message Image
	

Fig.2. "Pepper.png" image as cover image and "AED.tif" as the message image.

The algorithms defined by figure 3 and 4 are applied on the cover and message image set of figure5 that gives pertinent results of fig.6 where watermarking is carried out at various aspects. PSNR and NC variations show in fig.7 respectively.

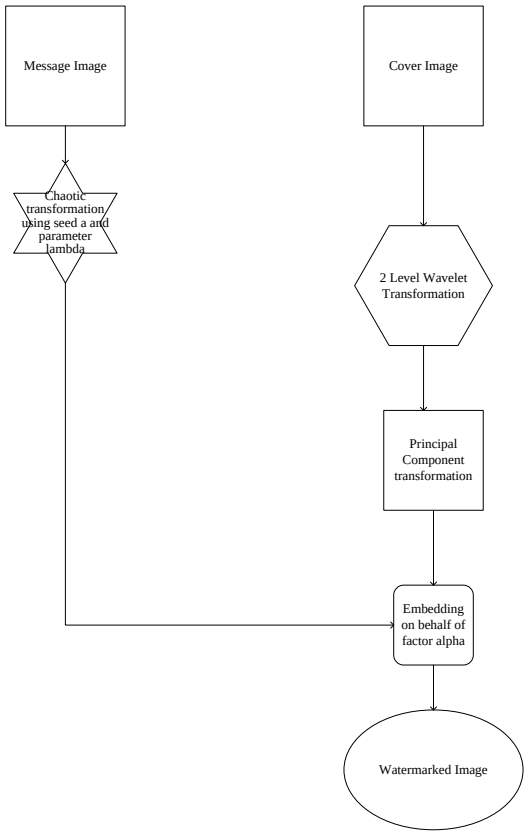


Fig 3. Flow graph of Embedding Algorithm

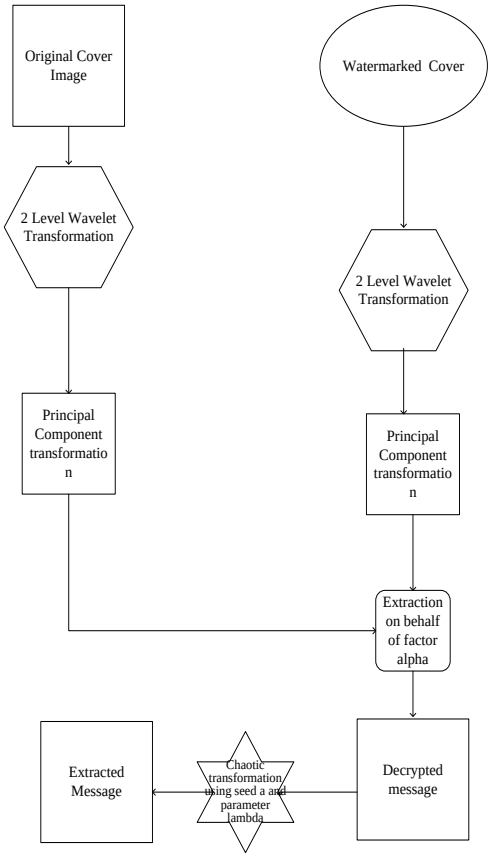


Fig.4 Watermark Extraction Flow graph

ISSN No: - 2456- 2165

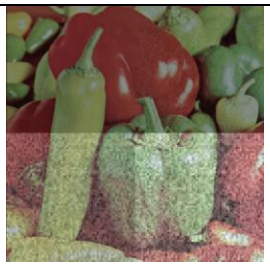
Wavelet Band	Watermarked Image
LL	
LH	
HL	
HH	

Fig. 5: The experimental outcome of watermarking carried out at various bands of Wavelet transformation.

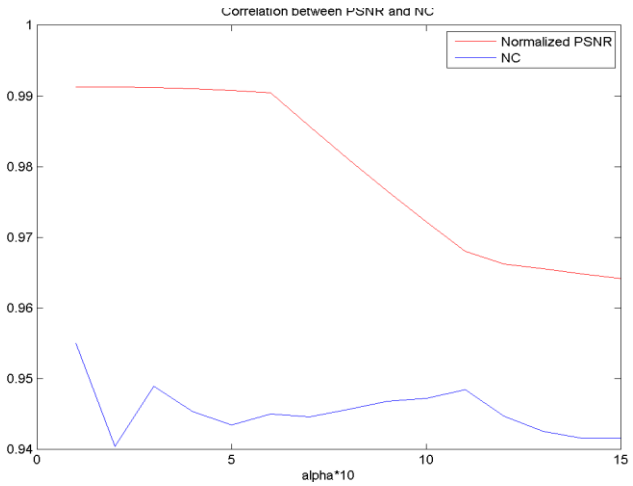


Fig.6. PSNR and NC plot depicting significant watermarking is achieved

VI. CONCLUSION

The art discussed in this article renders to information hiding using a bi-level security based algorithms deploying the chaotic mapping and multi resolution wavelet based approach. The experimental result proves that a significant level of performance is achieved using the proposed algorithm. Along with it this articles helps to suggest a range of hiding parameters so as to any ransom trivial applications of security parameters.

REFERENCES

[1] "Detection Of In-Situ Melanoma Using Symmetry Of Data And Color Spread Factor", International Journal Of Engineering Research, ISSN:2319-6890) (Online),2347-5013(Print), Volume No.3 Issue No: Special 2, Pp: 64-67.

[2] Petitcolas, F., Anderson, R., and Kuhn, M., "Information Hiding - a Survey." Proc. of the IEEE. Vol. 87, No. 7, (July 1999): pp. 1062–1078.

[3] Barni, M., Bartolini, F., Cox, I.J., Hernandez, J., and Perez-Gonzalez, F., "Digital Watermarking for Copyright Protection: A communications perspective." IEEE Communications Magazine. Vol. 39, No. 8, (August 2001):pp. 90–133.

[4] Langelaar, Gerhard C., Setyawan, I., and Lagendijk, R.L., "Watermarking Digital Image and Video Data: A state-of-the-art-overview." IEEE Signal Processing Magazine. Vol. 17, No. 5, (September 2000): pp. 20-47.

[5] Voyatzis, G., Mikolaides, N., and Pitas, I., "Digital watermarking: An overview." Proc. of IX European Signal Processing Conference(EUSIPCO), Island of Rhodes, Greece. (September 8-11, 1998): pp. 13-16.

[6] Wolfgang, R.B., Podilchuk, C.I., and Edward J. Delp, "Perceptual Watermarks for Image and Video." Proc. of the IEEE. Vol. 87, No. 7, (July 1998): pp. 1109-1126.

[7] Cox, I.J., Miller, M.L., and Bloom, J.A., "Watermarking Applications and their Properties." Proc. of IEEE Int. Conference on Information Technology, Las Vegas. (March 2000): pp. 6-10.

[8] Craver, S., Memon, N., Yeo, B.-L., and Yeung, M.M., "Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks and Implications." IEEE Journal On Selected Areas in Communications. Vol. 16, No. 4, (May 1998): pp. 573-586.

[9] Voloshynovskiy S. et al., "Attacks on Digital Watermarks: Classification, Estimation-Based Attacks, and Benchmarks." IEEE Communication Magazine. Vol. 39. No. 8, (August 2001): pp. 118-126.

[10] Gordy, J.D., and Bruton, L.T., "Performance Evaluation of Digital Audio Watermarking Algorithm." Proc .of 43rd IEEE Midwest Symposium on Circuits and Systems. Vol. 1, (August 2000): pp 456-459.