Digital Image Watermarking Using Optimization and Encryption

Hema Rajini N

Department of Computer Science and Engineering, Alagappa Chettiar Government College of Engineering and Technology, Karaikudi – 630003, Tamilnadu, India
auhemasmith@yahoo.co.in

Abstract—In this paper, with the technique of chaotic encryption-based blind digital image watermarking, we introduce a new grey wolf optimization. Discrete cosine transform (DCT) is employed before embedding the watermark within the host image. The image at host is split into 8x8 which is a non-overlapping blocks before employing DCT application, and the watermark bit is included through modifying the differences between the neighboring blocks DCT coefficients. Then, grey wolf optimization algorithm (GWO) is employed. Arnold transform is used along with the chaotic encryption to provide additional watermark security. The presented model is applied to a collection of benchmark images and the results validated the performance in terms of PSNR. The presented method attains maximum PSNR value on entirely given test images.

Keywords—Chaotic Encryption; Watermark; DCT; Stegnography

1. INTRODUCTION

For preserving intellectual protection rights (IPR) and content authentication, digital water marking is the optimal solution. It is the method of hiding the data in host media such as images, video and so on in a manner that it should not be notable to the human visual system (HVS). It make sure the data hidden security in video or image and play as a significant tool to look after different multimedia relating IPR problems. Anything like doctor signature, someone’s personal logo, institute logo and case history can be a digital watermark. Through different significant metrics such as payload, security, robustness and imperceptibility, the watermarking technique's efficiency is determined. If the image survives after processing attacks, a watermark is autonomous, that is from an attacked image, if an identifiable watermark is derived. Payload is the secret data bit counts which can be inserted into a host media that is given. When managing the host media quality, water is very unnoticeable if the HVS cannot recognize the watermark existence within host media. Even though an adversary derives the watermark, however, he cannot identify it without the encryption key, the watermark is secure. There present usually a tradeoff between the attributes as discussed through the conflict triangle [1] which is famous.

Depending on the watermark robustness degree towards attacks, the method of digital watermarking are segmented to three kinds: fragile, robust, and semi-fragile technique [2], [3]. In many operations of image processing, robust watermarks stays and it is highly appropriate for ownership verification and copyright protection, whereas the fragile watermarks disappear while media that is watermarked undergoes a little change and it is highly appropriate for integrity and authentication. In two varieties of domains, the watermarks are commonly embedded named as transform coefficient and pixel domain. In order to the watermark bits, the host image pixels are modified straightly in pixel domain watermarking. The method of pixel domain are simple to execute, and has lower computational cost and heavy payload. But, mostly the techniques of pixel domain offers lowest robustness. In order to the watermark bits, some transform frequency coefficients are modified in techniques of coefficient domain.

Numerous techniques of coefficient domain watermarking provide minimized payload and enhances robustness. For the techniques of coefficient domain watermarking, Discrete Cosine transform (DCT) and Discrete Wavelet Transform (DWT) are generally employed transforms. The techniques of coefficient domain and pixel domain are known as transform and spatial domain techniques. A
GA depended multiple watermarking methods using SVD and DWT has been given in [4]. Even though the method has been demonstrated as imperceptivity and robust, it comprise no provision of watermark security and the method is composite computationally. DCT is efficient as it gives a lower cost for hardware design over the different methods of transform domain. For DCT image computation, there exist usually three techniques. Either over the image block or over the entire images otherwise in DC coefficient image blocks, DCT is estimated straightly [5]. Through modifying the DCT coefficients, watermark embedding is performed in every technique.

Digital image DCT is classified extensively to three frequency coefficients bands. A watermark has to refuse many attacks for copyright protection and it is attained through embedding in lower frequency coefficients. As lower frequency coefficients comprise many image visual data, hence the coefficients changes might tend to lower quality of watermarked image. One might embed the watermark in high-frequency coefficients due to a little change to image will change the high-frequency coefficients through a little sum for authentication purposes. One might insert a watermark within the range of midfrequency, for the best solution of imperceptivity and robustness [6], [7].

The main concern about the methods of digital image watermarking is watermark security. A challenging factor for security purposes are the cryptographic methods mainly for image with medical and defense applications whereas the privacy is crucial attribute [8], [9]. Because of problems in redundancy and correlation, the tradition method of data encryption such as AES and DES and so on, have been demonstrated to poorly perform with digital images. At the same time, Chaos based encryption algorithms demonstrates effective outcomes because of the superior features like periodicity, ergodic nature, initial condition sensitiveness, and pseudorandom behavior. The chaotic methods adoption has been considered extensively because of the characteristics in the present years. Various techniques of image encryption have been projected with chaotic map [10]. In order to deal with the problem of security and IPR, various methods of watermarking are given. Most of the reviewed work aims at enhancing any one parameter among security, imperceptivity, computational efficiency, payload or robustness.

There exist no works which projects a best solution that can tend to an imperceptible, computationally efficient, secure, and robust technique to the best of the knowledge. This is because of the below things.

- Either no mechanism for security or worst encryption tool were used that might tend to security problems.
- Composite geometrical tool for the method of composite data hiding or image transformation has been used which might tend to computational complexity.
- For data embedding, the system fails to use or/and utilize a transformed image part. Few method employed huge block sizes which result to lower embedding capability.
- Altering the cover image pixels or low frequency coefficients through a huge sum might tend to lower imperceptivity.
- Altering the pixel or high frequency coefficients through a little amount, which result in lower watermark robustness to signal processing attacks.

Through projecting new watermarking method, we have attempt with best solution in this paper which takes into consideration the problems such as security, robustness, payload and imperceptivity and so on. The major work contribution includes:

- For embedding multiple or single watermarks, the methods is adaptive in order to the application requirement.
- For watermark embedding, inter-block coefficient correlation is employed in order to perform efficient payload and robustness.
Through modifying variance between two predefined DCT coefficients of two adjacent blocks, watermark bits are inserted. The alteration is performed by different geometric attacks and image processing are refused through creating the system autonomous.

For enhancing the security of watermarking, Arnold and chaos Nonlinear dynamics transform have been used.

In this paper, with the technique of chaotic encryption-based blind digital image watermarking, we introduce a new grey wolf optimization. Discrete cosine transform (DCT) is employed before embedding the watermark within the host image. The image at host is split into 8x8 which is a non-overlapping blocks before employing DCT application, and the watermark bit is included through modifying the differences between the neighboring blocks DCT coefficients. Then, grey wolf optimization algorithm (GWO) is employed. Arnold transform is used along with the chaotic encryption to provide additional watermark security. The presented model is applied to a collection of benchmark images and the results validated the performance in terms of PSNR. The presented method attains maximum PSNR value on entirely given test images.

2. PROPOSED METHOD

Fig. 1 demonstrates the projected watermarking system through an architectural representation. The two significant proposed subsystems are watermark embedding and watermark security unit. The unit of watermark security focus at improving the embedded watermark security to make it impracticable for an attacker to extract the accurate watermark even there exist a embedding algorithm knowledge. To attain a improved security, Chaotic theory and Arnold encryption is employed. In the below subsections, the preliminaries of geometrical of Arnold and Chaos are given.

A. Chaos and Arnold Encryption

For data encryption, chaotic based encryption method is an effective method. Irreversibility, dynamic behavior and pseudo-randomness are the qualities of Chaos signals. The system that has chaotic nature is highly sensible to primary parameters. The output chaotic sequence is similar as the white noise containing random feature with improved correlation and complexity and is expressed through:

$$C_{n+1} = \mu \times C_n \times (1 - C_n)$$  \hspace{1cm} (1)

Let $0 < \mu < 4$ naturally $\mu$ is given to rate 3.9 in order to attain enhanced randomness and $0 < C_n < 1$ is the nth rate produced from Eq(1). By modifying the $n$ value from 0 to L-1, different $C_n$ rates can be attained. The highest count of chaotic rates is given by L. We may retrieve the required chaotic signal, by assigning the initial rate of $C_0$ and $\mu$.

The chaotic encryption usage has been represented to offer improved security, it offers combined advantage of speed and security. Through employing different encryption methods, the data security might be improved and Arnold transform is also an efficient technique.
B. Watermark and Cover Generation

‘I’ refers the input image which is projected by the pre-processing unit as represented in fig. 1 and that for grayscale images plays as a buffer and for color images it act as converter. The pre-processing unit converts to YCbCr image the input RGB image to perform the watermark embedding to image luminance part wherever Y denotes the luminance data, Cb denotes chrominance blue data, Cr denotes chrominance red data.

When comparing with the chrominance data, the luminance portion ‘Y’ acts as watermark cover because of the image alteration in portions gives low notable modification towards the original image. If an individual need to insert three watermarks to a RGB image on the other hand one at each plane, pre-processing unit extracts the planes of RGB and sorts in a 2D matrix as the each plane might be P × Q grayscale plane, whereas the columns and rows of the cover image are denoted through Q and P correspondingly. Through subtracting 128, the resultant matrix rate are in the range of −128 to 127.

C. Justification about the parameters ‘µ’, and ‘c0’

Towards 1.35 to 3.9 range, the logistic parameter ‘µ’ is controlled as this ‘µ’ creates a chaotic rates with enhanced chaotic feature at 3.9 that gives enhanced security towards the watermark so that we selected ‘µ’ among 1.35 to 3.9. The primary rate of C0 might be among 0 and 1 so that we have selected through a key so as to enhance the watermark security.

D. Watermark Embedding

We have to insert encrypted watermark four bits for a provided 16 × 16 block, one among every DCT blocks pair that is demonstrated in fig. 2. The framework for bits ‘1’ and ‘0’ embedding is demonstrated in Fig. 2.
Fig. 2: Coefficient selection

Depending on the pre-embedding discrepancy between the two coefficients, ‘D’ is assumed as either zone 5 or zone 2 for bit hiding. The coefficients $C_{x+y+1}(k+1)$ and $C_{x+y}(i,j)$ are modified if the ‘D’ remains at zone 3 or 1 in order to that the variance between it gains to zone 2 that is the closest zone. When variance ‘D’ remains at zone 4 then the two chosen coefficients are changed in order that the variances attains to zone 5. Therefore, either the zone 5 or zone 2 will bear the bit ‘1’ data. Through changing the variances to the closest zone minimizes the image quality through a little sum when comparing with equivalent whereas the variance is changed to far zone. When the variance remains at zone 2, to embed bit ‘0’ then it is modified to zone 1, and it is modified to zone 4 when it stays at zone 5 or zone 3. It gives that bit ‘0’ data is saved at either zone 4 or zone 1.

Fig. 3: Sample test images

Through a 2S guard band, the various zones for certain bit are segregated wherever S is the strength at embedding that determines the projected watermarking system robustness. Towards the watermark, this guard band gives additional robustness. In the range of 5 to 20, S value has been selected. The system robustness is rational straightly to the S value, whereas imperceptivity is rational inversely towards S. Inverse DCT (IDCT) of every altered DCT blocks is estimated after completion of embedding as represented in Fig. 1. Through the operation of post-processing, IDCT is give that involve 128 addition towards every changed Blocks B*x elements in order that the
intensities of pixel varies from 0 to 255. When embedding luminance component, it involves conversion of YCbCr to RGB and resultant matrix is of three planes, for RGB plane embedding, three-color planes for watermarked color image are used. The post-processing operation completion gives final watermarked image.

E. Grey Wolf Optimization algorithm

Through the grey wolves hunting features, GWO algorithm is build in 2016. One among the top predators are grey wolves and survive in group of 5-12 wolves. The wolves are divided into beta, omega, alpha and delta based on the nature of hunting. The swarm actual leaders are alpha wolves which takes determinations relating to the hunting and place chosen to stay and it is known as dominant wolves. The rest of the wolves follow the dominant wolves orders. The next is beta wolf that take few determinations while the alpha dies. The next level wolves are known as delta wolves. The delta follows the order the above dominant wolves and the next level is omega. It act as scapegoat. The wolves hunting procedure is divided into (i) chasing and tracking (ii) following and encircling until the prey terminate movement and (iii) attack the prey. The symbols that are used for representations are delta ($\delta$), beta ($\beta$), and alpha ($\alpha$).

The prey encircling can be expressed as:

\[ D = |\hat{c}.X_p(k) - \hat{X}(k)| \]

\[ \hat{X}(k + 1) = \hat{X}_p(k) - \hat{A}.D \]

Let $k$ denotes the current iteration, $\hat{X}_p(k)$ refers the prey position vector, $\hat{X}$ refers the position vector, $\| \|$ denotes appropriate value and, is an element by element multiplication.

3. PERFORMANCE VALIDATION

The presented watermarking model is testing using a set of benchmark images as shown in Fig.3. Once the presented method is applied on a set of input images where the secret image is imposed on the cover image, the resultant image along with the input is shown in Fig. 4. To validate the performance of the presented method, PSNR is mainly employed to examine the visual resemblance of the input and the watermarked image. Root mean square error (RMSE) is utilized to identify the variations among the input image and the reconstructed image. PSNR is as

\[ \text{PSNR} = 20 \log_{10} \frac{255}{\text{RMSE}} \]

For indicating efficient performance and higher resemblance among two images, PSNR value must be high. Generally, the value of PSNR lies between 20 to 40. In case of no variation between two images, i.e. identical images, the PSNR will be $\infty$ and RMSE value will be 0.

Table 1 gives the assessment outcomes of the presented model on the applied collection of standard sample images. From the table, it is evident that attained PSNR value will be higher under the presented model over the compared ones. Fig. 5 also ensures that higher value of PSNR is attained by the presented method.
Fig. 4: Test images and their corresponding output image

The presented method exhibits maximum results on the entire given sample images. For example, for the image 4.2.03, the presented model shows higher PSNR rate of 39.28 whereas the traditional model obtains minimum PSNR value of 36.38. For the image 4.2.04, the presented model shows higher PSNR value of 37.89 whereas the existing model attains minimum PSNR value of 35.48. For the image 4.2.07, the presented model shows higher PSNR rate of 37.37 whereas the existing model attains higher PSNR rate of 35.48. For the image 5.1.12, the presented model shows maximum PSNR value of 35.27 whereas the existing model obtains minimum PSNR value of 34.28. For the image 5.1.14, the presented model shows higher PSNR rate of 35.27 whereas the traditional
model obtains minimum PSNR value of 34.28. For the image 5.2.08, the presented model shows higher PSNR value of 36.28 wherever the conventional model attains minimum PSNR value of 33.98. For the image 5.3.01, the presented model shows higher PSNR value of 38.27 wherever the conventional model attains minimum PSNR value of 32.39. For the image boat.512, the presented model shows higher PSNR value of 37.48 wherever the conventional model gains minimum PSNR value of 32.39. From the attained table and figures, it is proved that the presented method is superior to compared method in a significant way.

| Images  | Existing PSNR (dB) | Proposed PSNR (dB) |
|---------|-------------------|-------------------|
| 4.2.03  | 36.38             | 39.28             |
| 4.2.04  | 35.48             | 37.89             |
| 4.2.07  | 35.48             | 37.38             |
| 5.1.12  | 34.29             | 36.46             |
| 5.1.14  | 34.28             | 35.27             |
| 5.2.08  | 33.98             | 36.28             |
| 5.3.01  | 32.39             | 38.27             |
| boat.512| 35.90             | 37.48             |

Fig. 5: Comparative analysis of presented and existing model in terms of PSNR

4. CONCLUSION

In this paper, with the technique of chaotic encryption-based blind digital image watermarking, we have introduced a new GWO algorithm. DCT is employed in prior to embedding the watermark in the image at host. To validate the performance of the presented method, PSNR is mainly employed to examine the visual resemblance of the input and the watermarked image. The presented method
exhibits maximum results on the whole given test images. From the attained table and figures, it is proved that the presented method is superior to compared techniques in a significant way.

5. REFERENCES

[1] S. A. Parah, J. A. Sheikh, and G. M. Bhat, “On the realization of a secure, high capacity data embedding technique using joint top-down and downtop embedding approach,” Comput. Sci. Eng., vol. 49, pp. 10141–10146, Aug. 2012.

[2] C. C. Chang, P. Y. Lin, and J. S. Yeh, “Preserving robustness and removability for digital watermarks using subsampling and difference correlation,” Inf. Sci., vol. 179, no. 13, pp. 2283–2293, Jun. 2009.

[3] Z. Ni, Y. Q. Shi, N. Ansari, W. Su, Q. Sun, and X. Lin, “Robust lossless image data hiding designed for semi-fragile image authentication,” IEEE Trans. Circuits Syst. Video Technol., vol. 18, no. 4, pp. 497–509, Apr. 2008.

[4] N. Mohananthini and G. Yamuna, “Comparison of multiple watermarking techniques using genetic algorithms,” J. Electr. Syst. Inf. Technol., vol. 3, no. 1, pp. 68–80, May 2016.

[5] Q. Su, Y. Niu, Q. Wang, and G. Sheng, “A blind color image watermarking based on DC component in the spatial domain,” Optik-J. Light Electron Opt., vol. 124, no. 23, pp. 6255–6260, Dec. 2013.

[6] C.-T. Hsu and J.-L. Wu, “Hidden digital watermarks in images,” IEEE Trans. Image Process., vol. 8, no. 1, pp. 58–68, Jan. 1999.

[7] Y. K. Lin, “A data hiding scheme based upon DCT coefficient modification,” Comput. Standards Int., vol. 36, no. 56, pp. 855–862, 2014.

[8] K. Muhammad, J. Ahmad, H. Farman, Z. Jan, M. Sajjad, and S. W. Baik, “A secure method for color image steganography using gray-level modification and multi-level encryption,” Trans. Internet Inf. Syst., vol. 9, no. 5, pp. 1938–1962, 2015.

[9] K. Muhammad, M. Sajjad, and S. W. Baik, “Dual-level security based cyclic18 steganographic method and its application for secure transmission of keyframes during wireless capsule endoscopy,” J. Med. Syst., vol. 40, no. 5, p. 114, 2016.

[10] Y. Wang, K.-W. Wong, X. Liao, T. Xiang, and G. Chen, “A chaos-based image encryption algorithm with variable control parameters,” Chaos, Solitons Fractals, vol. 41, no. 4, pp. 1773–1783, 2009.

[11] Z ZAIN, “High Speed And Lowpower Gdi Based Full Adder”, Journal of VLSI Circuits And Systems, 1 (01), 5-9,2019

[12] NHK K. ISMAIL*, ”Estimation Of Reliability Of D Flip-Flops Using Mc Analysis”, Journal of VLSI Circuits And Systems 1 (01), 10-12,2019.