International Journal of Future Generation Communication and Networking
Vol. 13, No. 2s, (2020), pp. 521–526

Digital Image Watermarking by Using Discrete Cosine Transform Methodology

Kashmira Jagdale[1] ,Kanchan Pujari[2], Mahalaxmi Dudhanikar[3], Deeksha Gaikwad[4]

[1,2,3,4] *Dept. of E & TC Engg., Smt. Kashibai Navale College of Engineering, Savitribai Phule Pune University, Pune*

[1]*kashmira.jagdale27@gmail.com*
[2]*kapujari.skncoe@sinhgad.edu*
[3]*mahalaxmidudhanikar@gmail.com*
[4]*deekvingaikwad@gmail.com*

Abstract

Watermarking is the process of hiding the digital information in a carrier signal. The digital image watermarking approach for copyright protection is applicable to both RGB and monochrome images. Discrete Cosine Transform (DCT) is used for embedding the watermark in the host image. In the embedding process the luminance component of the host image is divided into 8 × 8 sub-blocks. By correlating the two DCT coefficients embedding can be implemented in DCT domain. Chaotic encryption is used to provide security with speed and efficiency. Arnold transform is used in addition to chaotic encryption to add double-layer security to the watermark. In addition it provides good hidden invisibility to the image and also prevents from several image attacks like joint picture expert group compression, sharpening, cropping and median filtering. The applications are like e-healthcare and telemedicine to robustly hide electronic health records in medical images.

Keywords— *watermarking, coefficient differencing, chaotic encryption, Arnold transform, DCT.*

I. INTRODUCTION

Internet has transformed the entire world into a global village. In recent years, there has been an extraordinary increase in sharing of digital data like text, images, audios, videos, etc. over it. However multimedia data is more prone to security risks as data can be hacked. According to the surveys across the globe, billions of money, thousands of jobs, etc. is risked due to security issues like copyright violations, piracy, unapproved production and marketing etc. To deal with such security issues the cryptography methodology has been chosen. Although cryptography has the potential to tackle these attacks but this methodology involves data modification visually and statistically. Digital watermarking is considered to be one of the best solutions for protecting IPR and content authentication.

Digital watermarking is a technique of hiding information in host media like video, images, etc., in a way that it cannot be noticed to human visual system (HVS). It ensures the security of the hidden images or data and prevents various multimedia related IPR issues. The digital image processing domain based digital image watermarking using chaotic encryption and Arnold transform has flourished as an effective methodology for security, authentication and copyright protection.

The study or techniques used to privately and securely transmit information with the presence of a third-party or adversary. Arnold transformation is applied widely in digital image scramble because of its periodicity. Arnold in the research of ergodic theory, it is also called cat mapping. The Arnold transform is a process of clipping and splicing that image part. Arnold transformation is a bi-directional and reversible and hence anti-Arnold transform can be applied to the image to get the original host image.

ISSN: 2233-7857 IJFGCN

II. LITERATURE SURVEY

Watermarking is a potential method for protection of ownership rights on digital audio, images and video data. In this paper, they have proposed watermarking scheme using techniques such as coefficient differencing and chaotic encryption in DCT domain. The main objective of this watermarking scheme is to provide security to the watermark. For the security purpose two methods known as chaotic encryption and Arnold transform are used which together provides double layer security to the watermark as well as offers joint advantage of speed and high resilience[1].

In this paper, they have explained about the watermarking technique in DCT domain using inter-block coefficient differencing. This scheme is highly robust against the image processing operations. The watermarking technique is based on inter-block coefficient differencing in which the difference between the two DCT coefficients of succeeding blocks at the same position decides the amount of modification needed to be done in order to embed the watermark bit.[2]

Watermarking can be done by combining DCT and DWT techniques. In this paper they have given the overview of watermarking technique using combination of DCT and DWT. In this combined algorithm, first of all the DWT of the image is calculated which results in four different image components of out which the watermark can be embedded on either horizontal or vertical component by calculating DCT. They have concluded that combined DCT-DWT algorithm provides better imperceptibility.[3]

In medical fields, authentication and confidentiality are the two most important factors. In order to maintain the privacy of the information, integrity and patient authentication a security technique based on watermarking and encryption is explained in this paper and it can be used for Digital Imaging and Communication in Medicine. They have used R-S-vector compression process for embedding the watermark. This technique is proved to be a totally revertible and it can retrieve the original images without any errors because of R-S-vector.[4]

Performance of watermarking algorithms are evaluated using different benchmarks. In this paper they have given the classification of various digital watermarks, Estimation-based attacks and benchmarks. Various watermarking attacks such as Removal attacks, Geometric attacks, Cryptographic attacks, Estimation based attacks are explained in detail. Also they have given overview of benchmark including estimation based attacks.[5]

Digital communication has become popular due to tremendous growth of internet. Cryptography and Steganography are the most popular techniques used for security purpose. In this paper, joint top-down and down-top embedding approach is used for data embedding. The results obtained from using joint top-down and down-top shows the better performance.[6]

A digital watermark is used as a valid solution to the problem of copyright protection for multimedia data in a networked environment. In this paper a low frequency watermarking with weighted correction has been proposed. In this technique watermarks are embedded into different position of the low frequency for each block. This method is resistant to some image processing operations and JPEG compression to some degree.[7]

There are numerous image scrambling algorithms are present such as Orthogonal Latin square, Affine transformation, Magic square, Knight Parade, Baker Transformation, Fibonacci Transformation etc. Among which Arnold transformation is used widely in digital image scramble due to its periodicity property. Arnold Transform is basically a process based on clipping and splicing which helps to realign the pixel matrix of digital image. Anti-Arnold transform algorithm has many advantages except it is time consuming when used in picture with big degree.[8]

Data hiding approaches are classified into two categories: the spatial domain and frequency domain. There are several approaches which are used to adjust the position and amount of embedding secret data. In this paper, they have proposed a steganographic scheme based on the ability of human vision which is insensitive to the varieties of high frequency components of image. They have used transform based approach which shows DCT coefficients has higher potential in competition with the pixel-value differencing method.[9]

A novel rank-based method for image watermarking is presented in this paper. This watermarking scheme uses only two DCT coefficients to hide one watermark bit in order to achieve high embedding capacity. This method is free of host signal interference.[10]

ISSN: 2233-7857 IJFGCN

The problem of period distribution of the generalized discrete Arnold cat map over the Galois ring is discussed in this paper. Hensel lift method is used to analyze the period distribution of the cat map over Galois ring.[11]

This paper illustrates about a new blind and robust image watermarking scheme based on Discrete Wavelet Transform and Discrete Cosine Transform. This scheme exhibits an acceptable good performance against various geometrical attacks and provides high robustness against various image processing attacks such as JPEG compression, noise adding, low pass filtering, sharpening and bit plane removal.[12]

Medical images requires security, confidentiality and integrity while transmitting. This paper presents a scheme which uses a part of sign sequence of DCT coefficients as the feature vector of images. Results of this scheme shows the high robustness as compared to other existing medical watermarking techniques.[13]

Image encryption helps to protect the confidentiality of the information. This paper represents visually meaningful image encryption scheme using Arnold Transform. This scheme uses Discrete Wavelet Transform in addition with the Arnold Transform. The final encrypted image produced using this scheme look similar to natural image and it will become difficult for the attacker to distinguish between encrypted image and natural image.[14]

III. METHODOLOGY

Multimedia security is extremely significant concern for the internet technology because of the ease of the duplication, distribution and manipulation of the multimedia data. The digital watermarking is a field of information hiding which hide the crucial information in the original data for protection illegal duplication and distribution of multimedia data. The image watermarking techniques may divide on the basis of domain like spatial domain or transform domain or on the basis of wavelets. The spatial domain techniques directly work on the pixels and the frequency domain works on the transform coefficients of the image. On embedding or data hiding a watermarked data is generated. Large numbers of watermarking schemes are currently available. An acceptable watermarking must possess certain qualities as robustness and imperceptibility.

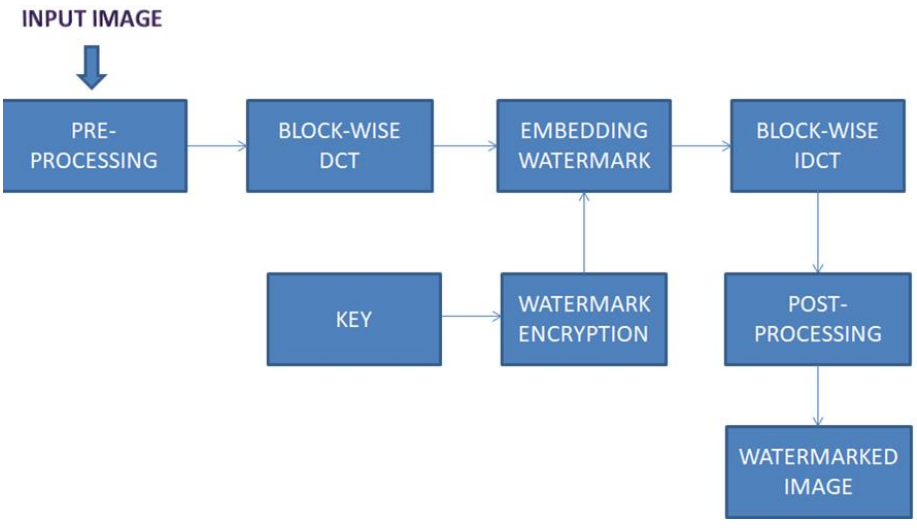

Figure 1. Block Diagram of Proposed System

IV. WATERMAKING TECHNIQUES

A. *Discrete Cosine Transform-*

The discrete cosine transforms is a technique for converting a signal into elementary Frequency components. It represents an image as a Sum of sinusoids of varying magnitudes and Frequencies.

ISSN: 2233-7857 IJFGCN

With an input image 'x', the DCT Coefficients for the transformed output image 'y', are Computed accordingly. The popular block-based DCT transform segments an image non-overlapping block and applies DCT to each block. This results in giving three frequencies Sub-bands: low frequency sub-band, mid-frequency sub-ban and high frequency sub-band. DCT-based watermarking is based on two facts. The first fact is that much of the signal energy lies at low-frequencies sub-band which contains the most important visual parts of the image. The watermark is therefore embedded by modifying the coefficients of the middle frequency sub-band so that the visibility of the image will not be affected and the watermark will not be removed by compression.

Input image: Output Image after DCT

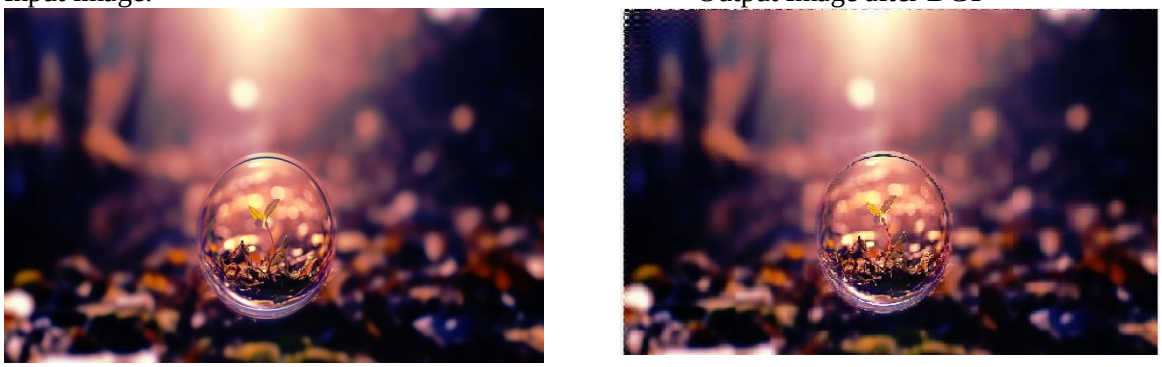

Figure 2. Effect of DCT algorithm on image

B. Coefficient Differencing-

For embedding watermark bit, the difference between two preselected DCT coefficients of two neighbouring blocks is calculated and is given as: D= Cxy(i,j)−Cxy+1(k,l) where (i, j) 6= (k, l), gives the position of the selected coefficient within a sub-block and $1 \leq i,j,k,l \leq 8$. x=1,2,3,4, ..., P/16×Q/16; whose value represents to which 16×16 pixel block the coefficient belongs while as y = 1,2,3,4 (whose value represents the 8×8 DCT block to which the coefficient belongs). From figure it is clear that for embedding first watermark bit the difference between coefficient is chosen from block Cx_1 and a coefficient from block Cx_2 is calculated. Similarly to embed the second watermark bit, the coefficients from block Cx_2 and the block Cx_3 and block C_{x4} are chosen for embedding fourth bit the blocks C_{x4} and C_{x1} are taken for different purpose. The difference 'D' is modulated according to the information bit to be embedded and the 'D'. The difference is varied in accordance with adding one coefficient and subtracting another coefficient by a value of Δ/2, where Δ is the amount of modification that needs to be brought between the two DCT coefficients iteratively until the difference reaches a particular zone.

C. Chaotic Encryption-

Chaotic encryption algorithm is most effective for data encryption. This algorithm is to be proposed by us in this paper. Signals involving in chaotic encryption algorithm possess qualities such as dynamic behaviour, irreversibility and pseudo-randomness. Chaotic nature systems are highly sensitive to initial parameters. Output of the chaotic sequence possesses property of random behaviour with highly improved correlation and complexity. The equation used for Chaotic encryption is- $Cn+1 = \mu \times Cn \times (1-Cn)$.

In above equation the value of μ is in between $0 < \mu < 4$ and it is typically set to '3.9' in order to achieve the highest randomness. By varying the values of parameter 'n' different values for Cn can be obtained. Initial values such as μ and C_0 can be set to a particular fixed value in order to get the required chaotic signal. Chaotic encryption offers advantages like high speed and increased security.

ISSN: 2233-7857 IJFGCN

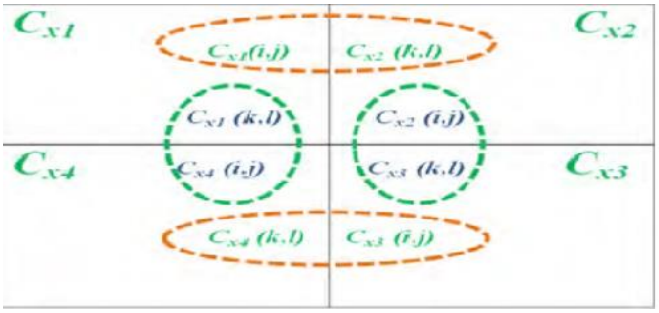

Figure 3. Chaotic Encryption

D. Arnold Transform-

Arnold transform is one of the most effective encryption technique in order enhance the security of information. This encryption method is two dimensional and works well for encryption of images of type N×N. The Arnold transformation is mathematically represented as-

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod} N)$$

here x and y are the co-ordinates of the pixel, N is the height or width of the square image processed, x' and y' are the coordinates of the scrambled image. The transform changes the position of two pixels, and if done for multiple times it will generate disordered image different from original image. Arnold encryption possess pseudo-random nature which results in highly secured scrambled image which cannot be hacked without knowing the sequence.

V. WATERMARK GENERATION

Watermark generation process starts with passing the input image through the pre-processing unit which acts as a buffer for grayscale images and as a converter for color images. To carry out watermark embedding into the luminance part of the image the pre-processing unit converts the input RGB image into YCbCr image, where Y stands for luminance information, Cb stands for chrominance blue information and Cr stand for chrominance red information of image. The luminance part 'Y' is put forward as cover for the watermark because modification of this part of the image brings less noticeable changes to actual image compared to the chrominance information. As well as if one wants to embed three watermarks into an RGB image, one in each plane, then the pre-processing unit extracts the RGB planes and then arranges all the three planes in a two-dimensional matrix so that each plane could be treated by the system as a P × Q grayscale plane, where P and Q respectively denote rows and columns of cover image. The resulting matrix values are brought in a range of −128 to 127 by subtracting 128 from the matrix. After pre-processing the resultant matrix is divided into 16×16blocks.Coefficient differencing technique is applied in order to brought the right amount of modification between 2 DCT coefficients. Before embedding the watermark two-level encryption of the watermark is performed in order to boost the security. The expected output after embedding the watermark using Chaotic Encryption And Arnold Transform is shown below:

Figure 4. Effect of embedding watermark using Chaotic Encryption and Arnold Transform

ISSN: 2233-7857 IJFGCN

VI. WATERMARK EMBEDDING

Watermark embedding is a process in which encrypted watermark is to be embedded in between each pair of DCT block. We are going to use 8 × 8 block for embedding four bits of encrypted watermark. We are going to use guard band for bringing the robustness in watermarking. The guard bands of 2S are going to be use where S represents the embedding strength. We are going to choose value of S in our project ranging from 5 to 20. Once the watermark is embedded, the next process we are going to do is IDCT which will convert YCbCr to RGB and conversion of resultant matrix into 3 planes which are basically three-color planes for watermarked color image in case of RGB plane. Once the post-processing operation concludes we will get the final watermarked image having double layer security.

VII. CONCLUSION

The experiment reveals that besides being resilient to singular attacks, it is highly resilient to combined attacks as well. The double layer of security of the embedded watermark ensures that it is highly secure in nature. We conclude that it is well suited for the application of copyright protection and ownership verification.

REFERENCES

[1] Nazir A. Loan, Nasir N. Hurrah, Shabir A. Parah, Jong Weon Lee, Javaid A. Sheikh "Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption" Department of Electronics and Instrumentation Technology, University of Kashmir, Srinagar 19006, India, Volume 6, 2018

[2] S. A. Parah, J. A. Sheikh, N. A. Loan, and G. M. Bhat, ''Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing'', Digit. Signal Process., vol. 53, pp. 11–24, Jun. 2016.

[3] Mr. V. P. Gohil, Prof. Ramlal, Yadav, Mr. D. G. Vaghela, "Digital Watermarking: Combining DCT and DWT techniques" ISSN:0975-6760 NOV 12 TO OCT 13 Volume-02,Issue-02

[4] M. M. Abd-Eldayem,''A proposed security technique based on watermarking and encryption for digital imaging and communications in medicine,'' Egyptian Informat. J., vol. 14, no. 1, pp. 1–13, Mar. 2013.

[5] S. Voloshynovskiy, S. Pereira, T. Pun, J. J. Eggers, and J. K. Su, ''Attacks on digital watermarks: Classification, estimation based attacks and benchmarks,'' IEEE Commun. Mag., vol. 39, no. 8, pp. 118–126, Aug. 2001.

[6] 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.

[7] S. D. Lin and C.-F. Chen, ''A robust DCT-based watermarking for copyright protection,'' IEEE Trans. Consum. Electron., vol. 46, no. 3, pp. 415–421, Aug. 2000.

[8] L. Wu and J. Zhang, ''Arnold transformation algorithm and antiarnold transformation algorithm,'' in Proc. ICISE, Nanjing, China, 2009, pp. 1164–1167.

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

[10] T. Zong, Y. G. Xiang, S. Guo, and Y. Rong, ''Rank-based image watermarking method with high embedding capacity and robustness,'' IEEE Access, vol. 4, pp. 1689–1699, 2016 .

[11] Fei Chen, Kwok-Wo Wong, Xiao feng Liao and Tao Xiang "Period Distribution Of The Generalized Discrete Arnold Cat Map for $N=2^{e"}$ IEEE Transactions On Information Theory, Vol. 59, NO.5, May 2013.

[12] A. Benoraira, K. B. Mahammed, and N. Boucenna, ''Blind image watermarking technique based on differential embedding in DWT and DCT domains,'' EURASIP J. Adv. Signal Process., p. 55, Dec. 2015, doi: 10.1186/s13634-015-0239-5.

[13] C. Dong, L. Jingbing, M. Haung, and Y. Bai, ''The medical image watermarking algorithm with encryption by DCT and logistic,'' in Proc. WISA, Haikou, China, 2012, pp. 119–124.

[14] Masilamani, ''An efficient visually meaningful image encryption using Arnold transform,'' in Proc. TechSym, Kharagpur, India, 2016, pp. 266–271.

ISSN: 2233-7857 IJFGCN