IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Traitement du Signal
Vol. 36, No. 3, June, 2019, pp. 233-237
Journal homepage: http://iieta.org/journals/ts

Image Transformation Technique Using Steganography Methods Using LWT Technique

Singamaneni Kranthi Kumar[1*], Pallela Dileep Kumar Reddy[2], Gajula Ramesh[3], Venkata Rao Maddumala[4]

[1] CSE Department, VNR Vignana Jyothi Institute of Engineering &Technology, Pragathi Nagar, Hyderabad, Telangana 500090, India
[2] CSE Department, SV College of Engineering, Karakambadi Road 517507, India
[3] CSE Department, GRIET, Bachupally, Hyderabad, India
[4] IT Department, Vignan's Nirula Institute of Technology & Science for Women, Guntur 522009, Andhra Pradesh, India

Corresponding Author Email: kkranthicse@gmail.com

https://doi.org/10.18280/ts.360305

Received: 7 March 2019
Accepted: 26 May 2019

Keywords:
embedding, steganography, extraction, texturization, watermarking

ABSTRACT

Digital image watermarking is a technique adopted to get rid of the increasing piracies in digital images. Computerized information can be effectively duplicated, altered and falsifications be made by anybody having a PC. Most inclined to such vindictive assaults are the watermarked pictures distributed in the Internet. Advanced Watermarking can be utilized as a device for finding unapproved information reuse and furthermore for copyright security. In the existing method, texturization dependant image watermarking methodology is performed which involves the embedding and extraction of a logo image to and from an original image respectively. After finding out the texture regions of host image, the logo image is embedded into the identified texture regions by Discrete Wavelet Transform. Before embedding, according to the textual characteristics of the host image analyzed, texturization of a logo is done by using Arnold transform and a rotation. It is effective for attaining a similar texture for both logo image and host image. Later the logo image is extracted back. Discrete Wavelet Transform results in degradation of quality and robustness of watermarked image. Also it is not a difficult task for an attacker to compromise the Arnold transform and rotation performed. In this work, Lifting Wavelet Transform technique is used instead of the Discrete Wavelet Transform as it overcome the above mentioned drawback. In addition, Arnold transform and rotation is replaced with circular shift method for enhancing security.

1. INTRODUCTION

Advanced Watermarking is the system of installing some distinguishing proof data known as watermark into the computerized information by its proprietor. On inserting or information stowing away a watermarked information is produced. Huge quantities of watermarking plans are right now accessible [1]. An adequate Watermarking must have certain characteristics as heartiness and indistinctness. Steganography and cryptography are the other methods used to hide the original message generally.

Steganography is used to embed message within another object by changing its properties. In cryptography, plaintext is converted to cipher text by using encryption key at sender side and other side receiver decrypt cipher text to plain text [2].

Watermarking techniques may be visible or invisible in nature. In visible watermarking, the watermark that we have embedded into the image is visible in nature whereas in later case, the watermark is not at all perceptible in nature [3]. Also watermarking techniques can be blind, semi-blind or non-blind in nature. The inception of information stowing away or undetectable watermarking might be followed to the time of old Greeks who moved their data in the wake of changing the substance in a content by swapping the places of letters in order. The Greeks consequently had the option to send mystery data over the fringe without getting took note.

There are existing methods which utilizes the techniques such as DCT, DWT [4], DFT etc. Also for ensuring more security, texturization on logo image is performed in some methods. In the existing method [5], texturization based image watermarking technique is performed which involves the embedding and extraction of a logo image to and from an original image respectively. After finding out the texture regions of host image, the logo image is embedded into the identified texture regions by Discrete Wavelet Transform [6].

Before embedding, according to the textual characteristics of the host image analyzed, texturization of the logo is done by using Arnold transform and a rotation [7]. It is effective for attaining a similar texture for both logo image and host image. Later the logo image is extracted back.

Discrete Wavelet Transform results in degradation of quality and robustness of watermarked image. Also it is not a difficult task for an attacker to compromise the Arnold transform and rotation performed [8]. In my work, I am using Lifting Wavelet Transform technique instead of the Discrete Wavelet Transform as it overcome the above mentioned drawback. In addition, Arnold transform and rotation is replaced with circular shift method for enhancing security.

Watermarking makes the duplications recognizable and in this manner reuse turns out to be practically unimaginable. For example the cash notes are watermarked by the legislature as confirmation for their credibility [9]. This makes phonies troublesome what's more, recognizable from the first. Another mainstream utilization of Watermarking is for sealing.

Therefore the robustness of watermark, computational efficiency increases, boundary artifacts, memory requirements and distortion gets reduces [10]. Aim of this research work is to ensure more security and quality in watermarking so that it overcome some drawbacks of the current technique [11]. Various researches on watermarking techniques are going on nowadays.

So a technique which overcome certain existing problems may be very useful for the future works. In this work, the watermarking technique by Arnold transform based logo texturization by Discrete Wavelet Transform scheme is implemented and checked the effectiveness of watermarking in this stage and finally enhanced the security of watermarking by using circular shifting and LWT technique thereby avoiding digital image piracies by ensuring ownership of images.

2. RELATED WORKS

Over the most recent couple of years, there have been numerous new and incredible steganography strategies revealed in the writing. These incorporate the spatial and the change space methods [12]. The benefits of the spatial area methods are their effortlessness and computational speed. The hindrance is their low capacity to hold up under the assaults i.e., they are less vigorous [13]. The change space methods have the upside of high capacity to confront the assaults i.e., they are increasingly hearty.

In the main level the mystery picture is covered up in DCT coefficients of one of the spread pictures and in the subsequent level, the stego picture of the principal level is installed in the subsequent spread picture utilizing LSB strategy. This strategy not just disguises the mystery message with improved security, yet in addition beguiles an aggressor [14]. In any case, the disadvantage is its intricacy and need for two spread pictures. One of things to come inquiries about referenced in this paper is to apply DWT rather than DCT to improve the security.

The best match is gotten by finding the base Root Mean Square Error (RMSE). This technique, which requires a great deal of calculations, did not separate the mystery information appropriately [15]. Two keys are utilized and the technique for transmitting them safely to the beneficiary isn't examined.

So as to guarantee lossless recuperation, the spread picture alteration is done before implanting. The inserting done on non-head corner to corner coefficients of the spread square guarantees better strength at the expense of the capacity [16]. The coefficients having vitality not exactly the edge is utilized for implanting. So as to shroud the discourse signals into discourse flag, the wavelet coefficients of the mystery messages are arranged and afterward concealed utilizing a roundabout LSB substitution [17].

3. PROPOSED WATERMARKING SCHEME

The watermarking process is performed by embedding the logo image into the host image by several steps. The texture and non-texture regions of the original image are calculated. Then texturization of the logo is performed by the circular shift method. Embedding the logo into the most matched textured host image block by comparing the HOG feature by lift ing wavelet transform is the next step. Then the watermarked image is obtained.

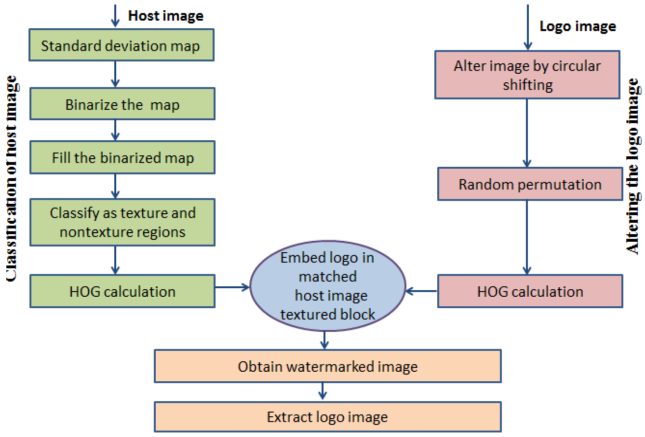

Figure 1. System design

For the most part computerized picture watermarking has certain necessities, the most significant being power and imperceptibility. Power implies that the implanted watermarks can't be expelled by purposeful or unexpected advanced information changing, called assaults. In spite of the fact that strength can be acquired dependent on critical alterations to the host information, such adjustments are observable and consequently don't fulfill the prerequisite of imperceptibility.

Since the discrete wavelet change permits free handling of the subsequent segments without critical discernible association between them, henceforth it is relied upon to make the procedure of subtle implanting increasingly successful.

The initial step is to ascertain a standard deviation map, signified by S. Here the standard deviation of each 3*3 square focused at position (x, y) is processed by the accompanying condition.

$$S(x,y) = \sqrt{\frac{\sum_{m=x-1}^{x+1}\sum_{n=y-1}^{y+1}(I(m,n)-\bar{I}_{xy})^2}{8}} \quad (1)$$

Here, moderately a high limit of 0.85 is connected.

This will abstain from setting the watermark in a blended locale containing something beyond surfaces.

$$\acute{S}(x,y) = \begin{cases} 1, & S(x,y) > \beta \max(S) \\ 0, & Otherwise \end{cases} \quad (2)$$

Hog component vector computation is performed for every single finished locale: Differences between the directions of the texturized logo and the host square impact the perceivability of the installed logo. For this, we register a histogram of arranged angles (HOG) for host picture obstructs here. Hoard is a component descriptor utilized for article discovery. It includes events of angle direction specifically limited parts or confined segments of a picture. Inclination of a picture speak to the directional change in force of a picture. Inclination move on from low to high qualities. Hoard figured as a thick lattice of consistently separated cells. For improved precision, it uses covering neighborhood standardization. Standardization procedure changes the scope of pixel force esteems to carry picture to a predetermined range.

Hoard technique incorporates slope calculation, direction binning and descriptor squares. Force angles depict the nearby item appearance and shape inside a picture. Picture is separated into little associated areas called cells. Histogram of angle bearings of pixels inside every phone are registered.

Descriptor is the connection of every one of these histograms. Bit of leeway of utilizing HOG descriptor is that it works on nearby cells. In this manner it opposes geometric changes. For improved exactness, differentiate standardization of nearby histograms should be possible. This can be performed by ascertaining a proportion of the power over a bigger area of picture called a square. Later by utilizing this worth, cells in a square can be standardized.

Perform texturization on logo picture by round move and irregular change: In this stage, the logo is roundabout moved by moving the last two bits to the principal position and moving the initial six bits to one side. At that point a change is performed haphazardly. The yield of this stage is the first texturized logo.

Hog component vector of texturized logo is determined: Compute a histogram of situated angles (HOG) for first texturized logo picture.

Find the ideal match of texturized logo picture with that of host picture by contrasting HOG include: The outright distinction between the HOG of the host picture squares and the first texturized logo picture are determined.

Hide the texturized logo into the coordinated surface area of host picture utilizing LWT: The logo picture is inserted into the host picture texturized district whose HOG coordinate the most.

From the past stages the finished squares of the hostblock alongside the first texturized logo is additionally acquired. A weight of 0.01 is connected for lessening the perceivability of watermark and to expand the watermark implanting quality. This weight worth controls the quality of inserting of logo in each finished host picture square. It is important to indicate the sub groups of the host picture in which the logo ought to be set. The implanting is performed by joining the sub groups of the logo picture with the comparing sub groups of the host picture, in a weighted design by applying the heaviness of inserting for expanding watermark subtlety.

Lifting wavelet change is a lossless picture pressure strategy which decreases the calculation time and quantizing blunders. As it is lossless, each single piece in unique picture can be recovered totally. It incorporates three activities split, anticipate and update. LWT isolates the picture into four sub groups as portrayed in the underneath segment.

The lifting wavelet change is performed to get the host picture sub groups LLh, LHh, HLh and logo picture sub groups LLl, LHl, HLl, HHl. HHh of every logo picture sub groups are implanted into the host picture sub groups and after that opposite lifting wavelet change is performed to recombine the sub groups.

$$\begin{aligned} LL_1 &= alp * LL_1 + LL_h \\ LH_1 &= alp * LH_1 + LH_h \\ HL_1 &= alp * HL_1 + HL_h \\ HH_1 &= alp * HH_1 + HH_h \end{aligned} \tag{3}$$

Obtain watermarked image.

Divide the different sub bands by the corresponding weight to obtain sub bands of the texturized logo. Apply the inverse lifting transform to the extracted logo sub bands to obtain the extracted logo image.

$$\begin{aligned} LL_1 &= LL_h - LL_1 / alp \\ LH_1 &= LH_h - LH_1 / alp \\ HL_1 &= HL_h - HL_1 / alp \\ HH_1 &= HH_h - HH_1 / alp \end{aligned} \tag{4}$$

4. FUNCTIONAL MODULES

The modules include

4.1 Standard Filtration and Dilation

Play out a division dependent on the nearby standard deviation and structure the standard deviation map. Parallel picture shutting with an organizing component of 9 pixel span plate is performed on the double guide. This aides in filling the openings and disengaged regions because of edge application inside the guide. In this manner double filled guide is acquired.

4.2 Texture calculation

Each block is classified as texture or non- texture region by setting a threshold.

A. Circular Shifting and Random Permutation

Logo is applied with Circular shifting and random permutation for acquiring the texturized logo.

B. HOG Feature Vector Calculation

HOG feature of texturized logo and the host block are calculated. Here differences and similarity between the orientations of the texturized logo and the host block are spotted.

C. Watermark Hiding

Logo image is embedded into the host image via LWT.

D. Extraction

Logo image and host images are extracted by the extraction process. This is the reverse process of embedding. Later the above modules of circular shifting and random permutation are replaced with Arnold transform and rotation followed by using DWT in the watermark hiding module. Performance is then measured by the structural similarity map for both cases. It is found that the first case shown better result than that of the latter case which used the discrete wavelet transform and circular shift. The result is checked for different logo images and host images.

5. RESULTS AND DISCUSSION

The performance analysis of my work is done by calculating the structural similarity map. The structural dissimilarity between the extracted logo and the original logo must be minimum. SSIM is used for measuring the similarity between two specified images. The structural similarity (SSIM) index is a method for predicting the quality of digital television, cinematic pictures, digital images and videos.

The SSIM index is a full reference metric. Prediction of image quality is based on an initial uncompressed image as reference. SSIM is proved to be better than traditional methods such as peak signal-to-noise ratio (PSNR) and mean squared error (MSE). These methods have proven to be inconsistent with human visual perception. Also PSNR and MSE approaches estimate absolute errors. But, SSIM is a perception based model. It considers image degradation as perceived change in structural information. The Binarized and filled map of the images are represented in Figure 2.

Figure 2. Binarized and filled map

SSIM incorporates important perceptual phenomena, including both luminance and contrast masking. The Textured and non-textured regions are represented in Figure 3.

Structural information is the idea that the pixels have strong inter dependencies especially when they are spatially close. These dependencies carry essential information about the structure of the objects.

Luminance masking is a phenomenon where image distortions are less visible in bright regions. Contrast masking is a phenomenon where image distortions become less visible where there is texture in the image. The watermarked image is obtained after embedding stage is perceptually similar to that of the host image in both the cases when used with circular shift, random permutation, LWT and with Arnold transform, rotation and dwt. Thus SSIM value is used for the analysis study.

First watermarking is performed by the lifting wavelet transform and circular bit shift. The structural similarity map of original logo image and the extracted logo image is calculated. Then the same is performed in case of discrete wavelet transform and Arnold transform. The first case shown better result when compared to the second case.

Figure 4 and Figure 5 shows the input host image and logo image respectively.

It is clearly understood that the structure of extracted logo image and original logo image of lifting wavelet transform and circular shift has shown a better value than those with discrete wavelet transform and Arnold transform. First has a SSIM value of 80.5558 whereas in second case, the map is not completely white and has a value of 72.6108.

The proposed method is applied for another three set of images also. Rather than the existing method, proposed method with lifting wavelet transform as embedding method and circular shift as texturization method shows a better reconstruction of the original logo.

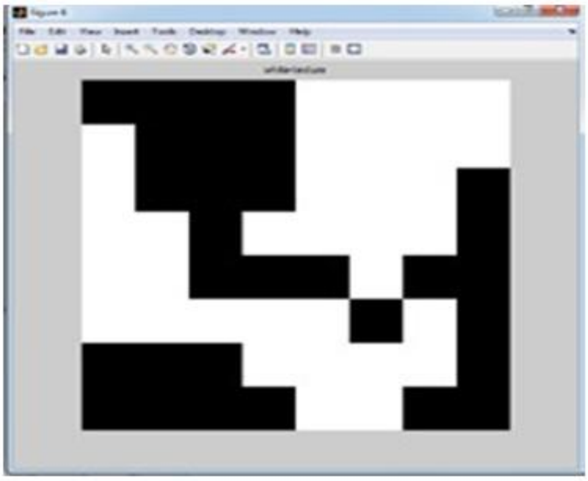

Figure 3. Textured and non-textured regions

Figure 4. Host image

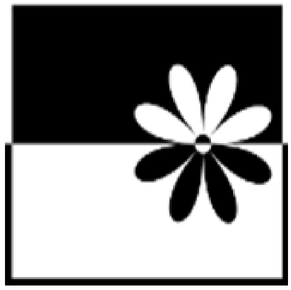

Figure 5. Logo image

6. CONCLUSION

A watermark is inserted into the host picture and we get the watermarked picture. Later for demonstrating the possession, this watermark is extricated from the watermarked picture and subsequently the host picture and watermark is gotten. Steganography and cryptography are different strategies used to shroud the first message for the most part. Steganography is used to embed message within another object by changing its properties. In this manuscript steganography techniques are used for enhancing security using, Lifting Wavelet Transform technique. The proposed exhibits better performance and the results show that the watermarking is done securely.

REFERENCES

[1] Ker, A.D. (2005). Steganalysis of LSB matching in grayscale images. IEEE Signal Processing Letters, 12(6): 441-444. https://doi.org/10.1109/LSP.2005.847889

[2] Shejul, A.A., Kulkarni, U.L. (2010). A DWT based approach for steganography using biometrics. IEEE International Conference on Data Storage and Data Engineering, pp. 39-43. https://doi.org/10.1109/DSDE.2010.10

[3] Bhattacharyya, S., Sanyal, G. (2012). A robust image steganography using DWT difference modulation (DWTDM). Int. J. Comput. Netw. Inf. Secur, 7: 27-40. https://doi.org/ 10.5815/ijcnis.2012.07.04

[4] Hamidi, H., Amirani, M.C., Arashloo, S.R. (2015). Local selected features of dual tree complex wavelet transform

for single sample face recognition. IET Image Process, 9(8): 716-723. https://doi.org/10.1049/iet-ipr.2013.0663

[5] Cunha, A.L.D., Zhou, J., Do, M.N. (2006). The non sub sampled contourlet transform: Theory, design, and applications. IEEE Transactions on Image Processing, 15(10): 3089-3101. https://doi.org/10.1109/TIP.2006.877507

[6] Gopi, A.P., Vejendla, L.N. (2017). Protected strength approach for image steganography. Traitement du Signal, 35(3-4): 175-181. https://doi.org/10.3166/TS.34.175-181

[7] Westfeld, A., Pfitzmann, A. (2000). Attacks on steganographic systems. Lecture Notes in Computer Science, Springer-Verlag, Berlin, 1768: 61-75. https://doi.org/10.1007/10719724_5

[8] Prabakaran, G., Bhavani, R. (2012). A modified secure digital image steganography based on discrete wavelet transform. Int. Conf. Computing, Electronics and Electrical Technologies, pp. 1096-1100. https://doi.org/10.1109/ICCEET.2012.6203811

[9] Dileep Kumar, G., Praveen Sam, R. (2018) Different security mechanisms in two-factor authentication for collaborative computing environment. In: Bokhari M., Agrawal N., Saini D. (eds) Cyber Security. Advances in Intelligent Systems and Computing, vol 729. Springer, Singapore. https://doi.org/10.1007/978-981-10-8536-9_3

[10] Singha, S., Sen, M. (2016). Encoding algorithm using bit level encryption and decryption technique. International Conference on Computer, Electrical & Communication Engineering (ICCECE), Kolkata, pp. 1-4. https://doi.org/10.1109/ICCECE.2016.8009584

[11] Li, X.F., Zhang, Y.H. (2016). Digital image encryption and decryption algorithm based on wavelet transform and chaos system. IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), Xi'an, pp. 253-257. https://doi.org/10.2415/AIMC.52411

[12] Kabi, K.K., Pradhan, C. (2014). Comparative study of image encryption using 2D chaotic map. IEEE Int. Conf. Information Systems and Computer Networks, pp. 105-108. https://doi.org/10.1109/ICISCON.2014.6965227

[13] Vejendla, L.N., Gopi, A.P. (2017). Visual cryptography for gray scale images with enhanced security mechanisms. Traitement du Signal, 35(3-4): 197-208. https://doi.org/10.3166/ts.34.197-208

[14] Kumar, V., Kumar, D. (2010). Performance evaluation of DWT based image steganography. IEEE 2nd Int. Advance Computing Conf, pp. 223-228. https://doi.org/10.1109/IADCC.2010.5423005

[15] Kurak, C., McHugh, J. (1992). A cautionary note on image downgrading. Proceedings of the Eighth Annual Computer Security Applications Conference, pp. 153-159. https://doi.org/10.1109/CSAC.1992.228224

[16] Lim, Wang, Q. (2010). The discrete shearlet transform: A new directional transform and compactly supported shearlet frames. Image Processing, IEEE Transactions, 19(5): 1166-1180. https://doi.org/10.1109/TIP.2010.2041410

[17] Mostafa, R., Ali, A.F., Taweal, E.G. (2015). Hybrid curvelet transform and least significant bit for image steganography. IEEE Seventh Int. Conf. Intelligent Computing and Information Systems, pp. 300-305. https://doi.org/10.1109/IntelCIS.2015.7397238