International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-9, Issue-1, January 2021
https://doi.org/10.21276/ijircst.2021.9.1.2
Article ID D10961, Pages 11-14
www.ijircst.org

Robust Digital Data Hiding in Low Coefficient Region of Image

Nomaan Jaweed Mohammed,[1] and Mohamed Manzoor Ul Hassan[2]

[1]Business Analyst, University of the Cumberlands, Naperville, Illinois, USA
[2]Business Analyst, Briggs & Stratton University of the Cumberlands Milwaukee, Wisconsin, USA

Correspondence should be addressed to Nomaan Jaweed Mohammed; email-id j.Nomaan@gmail.com

ABSTRACT- Digital images have many uses in the field of health, research, military, art, etc. Digital Images need annotation for retrieval and protection from piracy, attacks, and modification. To perform this retrieval and protection, some of the information was hidden in the image matrix. This paper proposes a data embedding and extraction algorithm. Low-frequency regions of the image are identified to embed secret information in LSV (Least Significant Value) and MSV (Most Significant Value) of a selected coefficient once the data hiding in the embedding section of the proposed model image gets retransformed in the original image structure as per the number of bits used in LSV and MSV for data hiding image gets secured from different spatial attacks. The experiment is performed on real images. A comparison of the proposed model is done on PSNR, MSE, evaluation parameters. It is shown that the proposed model is better as compared to the existing model.

KEYWORDS- Data Hiding, DIP, Information Embedding, Information Extraction, LSB, MSB.

I. INTRODUCTION

As the digital world is growing, people are moving towards different services provided by it. Some of these services are social networks, e-commerce, etc. But this technology gives rise to the new problem of piracy or in other words proprietary get easily stolen. So, to overcome this, different techniques are used for preserving the proprietorship of the owner. One such digital approach is cryptography which in other words is hiding information that is used to put some information in the original image which will specify the originality of the digital data like photographs, digital music, or digital videos [1, 2]. One of the basic causes of the copyright issue is the ease of availability of the internet and software that can modify the content as per the user requirement. With an increased concern in copyright protection, comes an increased interest in digital watermarking. The internet, for the most part, is a user-friendly place where people are interested in downloading pictures, music, and videos. The internet provides an efficient delivery system that is relatively inexpensive. Acquiring media via the internet requires a fraction of the time it would take to go to a physical store to purchase said media. Also, when one purchases media over the internet, one would only need virtual space to store the media in question as opposed to storing it on a shelf or wherever such media might be placed [3]. Conversely, such ready availability provides people with the possibility of copyright violations. If one were to visit any store that specializes in technology, one can acquire a plethora of digital recording devices. Back when the average customer could only acquire analog recording devices at great cost, the quality of such recordings did not compare to the quality of the original. Conversely, the ready availability of digital recording devices can produce a duplicate with little loss in quality. The combination of these digital recording devices and the internet has provided individuals with the opportunity to rapidly distribute copyrighted material without appropriate compensation to its owners [4, 5]. Ergo, owners of various media are interested in technologies that can provide adequate protection to their products. The technology that media owners apply to protect their content is cryptography. Since cryptography was used, this is the most common method for protection as well as the most developed. The collection of files would be encrypted using an encryption key. The files would then be distributed to paying customers. Finally, the customer would use a decryption key, provided by the distributor, to access the set of files. The risk of someone acquiring the set of encrypted files is considered acceptable, provided that the decryption key is only available to paying customers. However, what is to stop the paying customer from distributing the set of files once it has been decrypted? Once the paying customer acquires the decryption key, that customer can then distribute the set of files at will via the internet. In other words, while cryptography can protect files from interception, the technology will not protect files from the end-user.

II. RELATED WORK

In [6] the author has proposed a Singular value Decomposition technique to find resemble data in the original image. The authors of this paper divide the image into fix size patch and replace those patches with KSVD patch. This increases the image security in the network while encryption of the watermark was also done before embedding. Here, searching for the correct patch from the KSVD library was time-consuming. Dictionary storage at the sender or receiver side

was also bulky. CNN was used for embedding the watermark data in the original image. With the help of some supporting information, it was found that Watermarking was extracted from the image. Here, it was established that both watermarking and image got reversed at the receiving end.

Huang et al. [7] has proposed a novel blind watermarking technique using Back Propagation neural network in wavelet domain. In this paper, a scrambled watermark is embedded using the advantage of Human Vision System (HVS) to achieve better imperceptibility and robustness. Neural network is used to memorize the relation between the embedded watermark and the corresponding watermarked image.

Peng et al. [8] have proposed a novel image watermarking technique in the multi-wavelet domain based on SVM. The algorithm has utilized a special frequency band and the property of image for watermarking. Though the scheme is reasonably robust against various attacks, it fails to achieve robustness against average filtering, median filtering, JPEG attacks, and scaling attack effectively. Yang et al. [9] has also proposed a robust technique in the undecimated discrete wavelet transform (UDWT) domain using fuzzy SVM for geometric distortion correction. Though the technique provides adequate robustness, it requires excessive computational time and is also not robust to local geometric distortions. In [10] Third-level LFT (Lifting Fourier transform) is used for embedding watermark. Feature set generated from the blocks in which reference watermark RW was embedded has been used as an input feature vector in Feed-Forward neural network. The corresponding bits of RW are used as the target vector. The technique provides satisfactory robustness against different attacks such as noising attacks, de-noising attacks, some geometric attacks, etc. In [12] a robust and reversible database watermarking technique, Genetic Algorithm, and Histogram Shifting Watermarking (GAHSW) are proposed for the numerical relational database. The genetic algorithm is used to select the best secret key for grouping database, where the watermarking can be embedded with balanced distortion and capacity. The histogram of the prediction error is shifted to embed the watermark with good robustness. Histogram shifting reduces the robustness of the work.

III. PROPOSED METHODOLOGY

In this section proposed work explanation is done which focuses on embedding and extraction of data in a cover image. The entire work is done in two stages - the first is the embedding of data and the second is the extraction of digital information. It is desired that while extracting secret information the whole data remains secure. In Fig. 1 entire proposed work block diagram is clarified.

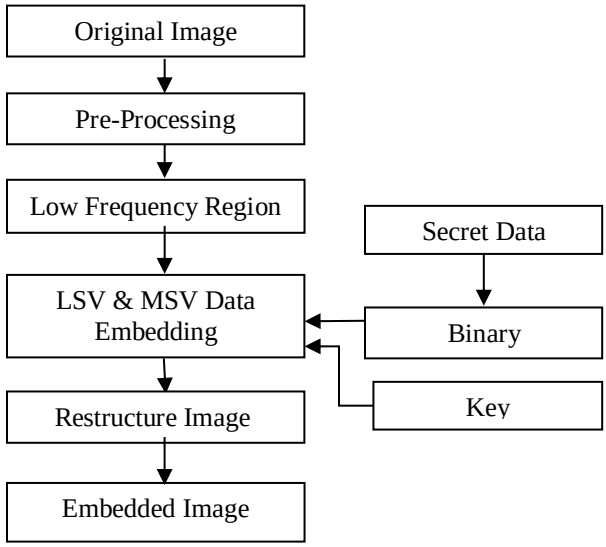

Fig.1: Block diagram of proposed work.

A. Pre-Processing

Image is a matrix of pixel values having a fixed range as per the selected format of the image. Format like the color image has 0-1, gray has a 0-255-pixel range where 0 is black and 1 or 255 is white. So as per the working environment of the proposed model, the image gets transformed in two dimensions format. As the whole work focuses on the image which has pixel value in the range of 0-255, pre-processing an image implies making a matrix of the same.

B. Low-Frequency Region

In this section of the proposed model, low-frequency feature values are extracted from the image. The image gets transformed into the frequency domain bypassing the image matrix through a series of low pass and high pass filters. The output from the two consecutive low pass filters of an image is considered a low-frequency region feature of the input grayscale image.

C. Secret Data Pre-Processing

Input secret data either text, number, the image gets transformed into corresponding ASCII number where each ASCII number gets is converted into an 8-bit binary number. So, this conversion of data into its ASCII binary format is the pre-processing step of this proposed model. All set of binary information is stored in a single vector.

D. LSV & MSV Data Embedding

Low-frequency feature values are converted packets of T number of coefficient and as per secret data binary vector bit LSV (Least Significant Value), MSV (Most Significant Value) is modified for embedding. This work creates a difference between LAV and MSV as per binary secrete data. Let for binary bit 1, check if MSV was lower than LSV, then interchange each value by position. Similarly, for secret binary bit 0, check if MSV value was lower than LSV, then interchange each value by its position. This interchange

reduces embedding modification and maintains the quality of the image. Embedding in one or two or three-position acts as Key in embedding.

E. Restructure Image

Once the secret binary information bits are embedded into the low-frequency feature region, the embedded low-frequency region was recombined with another region of the image. All frequency regions were retransformed back to their original pixel value range.

F. Extraction of Image

In this extraction step, the receiver can extract data and images by using the above block diagram. This segment of the proposed work is for picture extraction at the recipient side. The low-frequency feature again extracts and converts into a packet of T number of the coefficient which is a further process to compare the LSV and MSV. As per the comparison, if LSV values are high then consider 0 binary secret information, and if MSV values were high, then consider 1 binary bit. If Key-value was more than 1 then the majority of 0 or 1 was considered as the final secret information from that packet.

IV. EXPERIMENT AND RESULTS

This section exhibits the experimental assessment of the proposed procedure for the protection of the picture. All calculations and utility measures are executed by utilizing the MATLAB apparatus. The tests are performed on a 2.27 GHz Intel Core i3 machine, outfitted with 4 GB of RAM, and running under Windows 7 Professional.

A. Dataset

The analysis is done on the standard pictures, for example, mandrilla, lena, tree, and so forth. These are standard pictures that are gotten from http://sipi.usc.edu/database/?volume=misc. The framework is tried on everyday pictures too.

Evaluation Parameter:

Peak Signal to Noise Ratio

$$\text{PSNR} = 10\log_{10}\left(\frac{Max\_pixel\_value}{Mean\_Square\_error}\right)$$

Mean Square Error

$$MSE = \frac{\sum_{i=1}^{n}(X_{obs,i} - X_{model,i})^2}{n}$$

Where X_{obs} is the original cover image pixel values and X_{model} is the extracted image. The smaller the means average error, the closer to the ground truth values.

Normalized Correlation: Normalized Correlation (NC) The Normalized Correlation (NC) between the images WM and EM which are of size m x n is given by the following expression. Its value ranges in the interval [0 1], closer to the NC value to 1, higher is the correlation between the two images.

B. Result

Table 1: PSNR Based Comparison between proposed and previous work

PSNR Based Comparison		
Images	**Proposed Work**	**Previous Work**
Tree	32.5956	2.26785
Lena	36.0512	3.20154
Bowl	26.9851	5.49349

From table 1 it is obtained that under ideal conditions the proposed work is better as compare to previous work in [13]. under PSNR evaluation parameters. As DWT and histogram shifting algorithm has regenerated images in color format, this parameter is high as compared to the previous value.

Table 2: MSE based comparison between proposed and previous work

MSE Based Comparison		
Images	**Proposed Work**	**Previous Work**
Tree	35.7699	38574.1
Lena	16.1422	31111.9
Bowl	130.187	18354

From table 2 it is established that under ideal conditions, the proposed work is better in comparison to the previous work in [13] under MSE evaluation parameters. As DWT and histogram shifting algorithm has regenerated images in color format, this parameter is high as compared to the previous value.

Table 3: Executing Time (Seconds) based comparison between proposed and previous work

Embedding Time (Seconds) Based Comparison		
Images	**Proposed Work**	**Previous Work**
Tree	11.5568	3.37464
Lena	10.2342	2.87481
Bowl	10.2386	2.74852

From table 2 it is established that under ideal conditions the proposed work is better as compared to the previous work in [13], under MSE evaluation parameters. As DWT and histogram shifting algorithm has regenerated images in color format. this parameter is high as compared to the previous value.

Table 4: Extraction rate comparison between proposed and previous work

Filter Attack Based Data Extraction Comparison		
Images	**Proposed Work**	**Previous Work**
Tree	0.773	0.691
Lena	0.787	0.681
Bowl	0.698	0.651

From table 4 it is obtained that under filter attack conditions, the proposed work is better in comparison to the previous work in [13]. NC evaluation parameters. As DWT and histogram shifting algorithm has regenerated images in color format, this parameter is high as compared to the previous value.

Table 5: Extraction rate comparison between proposed and previous work

Salt & Pepper Attack Based Data Extraction Comparison		
Images	**Proposed Work**	**Previous Work**
Tree	0.865	0.67
Lena	0.822	0.672
Bowl	0.883	0.657

From table 5 it is established that, under noise attack conditions, the proposed work is better as compared to the previous work in [13]. Extraction rate evaluation parameters. As DWT and histogram shifting algorithm has regenerated images in color format, this parameter is high as compared to the previous value.

VI. CONCLUSIONS

Digital information is developed by investing time and money but easy steps of piracy lead to waste of this labor as numerous algorithms are proposed for preventing and claiming the ownership of digital content like image and video. In this work, the digital image data hiding is done by extracting the low-frequency region of the image. As per key-value LSV and MSV of extracted feature packets were modified for secret binary information embedding. The use of LSV and MSV concept for embedding reduces the information losses in the image. Different real image dataset is used for experimental purposes. The result shows that the proposed model performs well in an ideal and attack environment. In the future, research can be performed on embedding in video and audio files.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

[1] Priya Porwal1, Tanvi Ghag2, Nikita Poddar3, Ankita Tawde Digital Video Watermarking Using Modified Lsb And Dct Technique. International Journal of Research in Engineering and Technology eISSN: 2319-1163.

[2] Kazuki Yamato, Madoka Hasegawa, Yuichi Tanaka‡ and Shigeo Kato. "DIGITAL IMAGE WATERMARKING METHOD USING BETWEEN-CLASS VARIANCE". 978-1-4673-2533-2/12/$26.00 ©2012 IEEE.

[3] Ashwary Rajpoot, Ranjana Batham, Navin Chourasia "Spatial Domain base Image Watermarking by Edge Features". IJCSEC-International Journal of Computer Science and Engineering Communications. Vol.2, Issue 5, Oct 2014, ISSN: 2347–8586

[4] Mr. Mohan A Chimanna 1, Prof.S.R.Kho "Digital Video Watermarking Techniques for Secure Multimedia Creation and Delivery" Vol. 3, Issue 2, March -April 2013, pp.839-844839.

[5] Paweł Korus, Student Member, IEEE, and Andrzej Dziech. "Efficient Method for Content ReconstructionWith Self-Embedding". IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 22, NO. 3, MARCH 2013.

[6] HaniehKhalilian, Student Member, IEEE, And Ivan V. Bajic Video "Watermarking With Empirical PCA-Based Decoding" Ieee Transactions On Image Processing, Vol. 22, No. 12, December 2013.

[7] S. Huang, W. Zhang, W. Feng and H. Yang, Blind watermarking scheme based on neural network, Proceedings of the 7th IEEE World Congress on Intelligent Control and Automation (2008), 5985–5989.

[8] H. Peng, J. Wang and W. Wang, Image watermarking method in multiwavelet domain based on support vector machines, Journal of Systems and Software 83(8) (2010), 1470–1477.

[9] H.Y. Yang, X.Y. Wang and C.P. Wang, A robust digital watermarking algorithm in the undecimated discrete wavelet transform domain, Computers and Electrical Engineering 39(3) (2013), 893–906.

[10] MohiulIslama,∗, AmarjitRoyb and RabulHussainLaskar. "Neural network based robust image watermarking technique in LWT domain". Journal of Intelligent & Fuzzy Systems 34 (2018) 1691–1700.

[11] Ahmed A. Abd El-Latif, BassemAbd-El-Atty, M. Shamim Hossain, Md. Abdur Rahman, AtifAlamri, B. B. Gupta. "Efficient quantum information hiding for remote medical image sharing". Digital Object Identifier 10.1109/ACCESS.2017.

[12] Donghui Hu, Dan Zhao, ShuliZheng. "A New Robust Approach for Reversible Database Watermarking With Distortion Control". IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, 2019.

[13] Qingtang Su, Decheng Liu, Zihan Yuan, Gang Wang, Xiaofeng Zhang, Beijing Chen, And Tao Yao. "New Rapid and Robust Color Image Watermarking Technique in Spatial Domain". IEEE Access March 25, 2019.