I.J.Computer Network and Information Security, **2014,1, 34-38**
Published Online November 2013in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2014.01.05

An Efficiency and Algorithm Detection for Stenography in Digital Symbols

Takialddin A. Al Smadi[1],Mohammed Maitah[2]
[1]Department of Communications and Electronics Engineering,
College of Engineering, Jerash University, Jerash-Jordan
dsmadi@rambler.ru
[2]Computer Science Department, King Saud University, Riyadh, KSA

Abstract—in modern conditions; Steganography has become the digital strategy of hiding files in one form or other MEDIA like images, sound files or video files. Algorithms built-in digital information for color images based techniques steganography. This work presents a new method of steganography based on space domain to encode more information in the image, making small changes in their pixels. The results work obtained in this work that the new detection method of steganography based on new spatial coding additional information in the image, making small changes in their pixels based on the expansion of the range is designed for testing the proposed structure. This work study is to develop a new method to detect human faces, reflected in digital photography, with a high work rate and accuracy of detection.

Index Terms—Embedded System, Steganography, Digital image, Information symbol

I. INTRODUCTION

The problems of object detection on digital picture are very challenging one due to rapid development of photo-and video electronics.

Despite the fact that physical reality contains a lot of different objects, the development of detection algorithm for a more narrow class of objects - human faces - is of considerable interest due to the increasing degree of automation of various processes and production systems, thus the particular application of the algorithm of human faces detection may be as follows:

The algorithm of human faces detection may be as follows methods:

1-Automatic registration of visitor's number in the supermarkets and entertainment centers.

2-In crossing control systems in various institutions, airports, subway;

3-Automated systems to prevent accidents, they monitor the face of vehicle's Driver man-machine intelligent interfaces [1]. The current requirements for setting up such systems impose strict limits on the speed of execution algorithms, which shall operate in real time mode. Hence, the perspective problems to be solved are creation of fast and reliable algorithm of human faces detection.

Available approaches to face detection problem.

Over the past 10 years, the dynamic development are carried out in the area of detection of the image and were offered various detection methods, principal component analysis, using the histogram, neural networks, Bayesian Networks, statistical methods, etc. some of these detection algorithms are invariant with respect to the object, while others use such a priori knowledge about the object, such as a form, the colors, the relative position of parts [2]. The work is to develop a new method to detect human faces, reflected in digital photography, with a high work rate and accuracy of detection [3].The algorithm was adopted as the basis of the new method. All found flaws in the algorithm, and the use of a priori knowledge on the shape and color of a person's face made it possible to identify possible ways to improve the performance of the algorithm and a new method to detect the faces of the people, Digital steganography science secure communication, which is often done through the introduction of a digital object in the normal message, modifying it. Embedding the result is transferred to the recipient, which retrieves an embedded message. This is an effective way to protect information that is particularly relevant in the case of secret key, steganography, using conventional publicly known algorithm and secret key in advance the selected connection both sides [4]. This option must be either blind insertion or retrieval of information, and if the correct key is not used, it cannot be known if the data is actually hidden in the object [5]. If security or, if you prefer, you cannot be hidden secret key before connection hidden links, another feature of the public key steganography. It entails a sender by using the recipient's public key to embed information that can only be detected by using the private key of the recipient. It works the same way as the public key infrastructure. An interesting feature of the public key steganography is that even the sender should not be able to find the secret message by steganography. Alternatively offers the key exchange protocol of steganography, where communicating parties share a sequence of messages that look like a normal conversation and at the end of the sequence, each of the parties may calculate the key. The key may be the least can then be used for

steganography secret key. Regardless of how it is steganography is not useful if it can be proven the existence of classified information by external parties [5]. Deer analysis is the method by which you can determine the presence of a hidden message and try to determine the true content of the message. Digital steganography due to hidden digital watermarks, but watermarks often uses fewer messages and has different goals often copyrighted, to some extent, they are interchangeable. There is special software for the practice of digital steganography, and this can allow hiding messages in digital watermark, although other methods may be more common, some digital steganography software better than other in effectively hiding messages [6].

The new method can detect on steganography based on new spatial coding additional information in the image, making small changes.

In their resolution, based in connection with the expansion of the range is designed for the testing of the proposed structure.

Organized by the main content of this document is to develop a new method to detect human faces, reflected in digital photography, high speed and accuracy of detection. The algorithm was adopted as the basis of the new method. All found flaws in the algorithm, and the use of a priori knowledge on the shape and color of a person's face made it possible to identify possible ways to improve the performance of the algorithm and a new method to detect the faces of the people.

Digital Steganography

General model for steganography is set for an arbitrary connection channels, only those where the MEDIA coverage consists of multimedia objects such as images, video or audio files, have practical value.

This is so for three reasons: first, the cover object must be larger than the secret messages. Even the most famous implementation methods do not allow us to introduce more than 1% of the size of the cover securely. Uncertainty in the lid is necessary to achieve the security of steganography. Large objects without uncertainty, for example, the mathematical constant π with very high accuracy, are inappropriate, because the Superintendent would be able to check out their regular the structure and detect traces of embedding. Data transfer, contains ambiguities need to be plausible. Image and audio files so vitally currently, communication media transferring such data is imperceptible. As in modern cryptography, it is common to assume that the Kerckhoffs principle It is listened to in digital steganography. Principle States that algorithm of steganography to embed secret messages in and unpack it the lids should be public. Security is achieved only through the secret keys, shared communication partners Simmons anecdote: agreed after before being locked up). However, the right interpretation of this principle for the case of steganography is not always easy, as the steganography may have additional degrees of freedom. For example, select the cover does not have a direct equivalent in standard cryptographic systems. Figure 1 shows the baseline scenario for digital steganography following the terminology laid down It depicts two parties, sender and recipient,

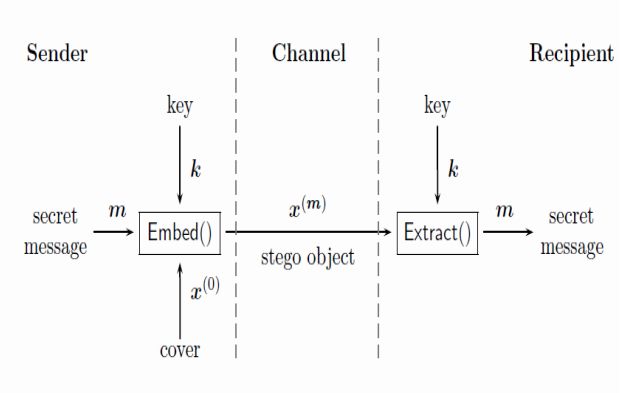

Figure.1: Block diagram of baseline steganography System

II. RELATED WORKS

Simulation of Digital Image Watermarking tasks outlined in the Insert watermark detection is similar to the information in the message and serting detection systems. Watermark in the formation is that the sender intended to send a signal to a receiver on the other end of the communication system, the watermark, has invested in his career, the original image is watermarked images can be saved or passed on to, and can even be modified or corrupted. On the receiver side, you can find the watermark information can damage the image watermark. The watermark is shown in Figure 1. That this technology for evolved throughout history [7].

Select the image container, channel, where the transmitted images with built-in characters added additive noise, blocks the formation of the message. The method of pixel by pixel filtering of image, Pixel image filtering method is a series of filtering the display function. Each pixel of the original image depending on its intensity and the intensity of his neighbor corresponds to a certain value. The purpose of such filtration is to separate the regions that do not contain face's areas, the information about distribution of values of the target object show that Figure 2.

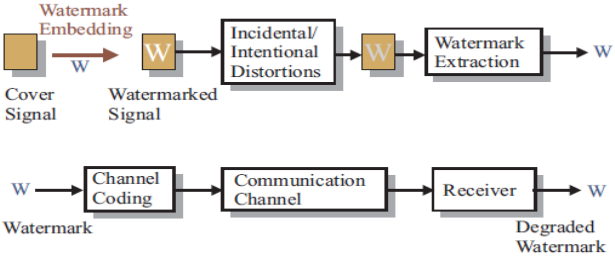

Figure.2: Communication system model for watermarking problems

This is a replacement of character sequences in the pseudorandom sequence (PRS) and the introduction of information in an image, if the current embedded character bit is 0 it uses not inverted pseudorandom sequence, and the inverted value of 1 character. The CAP length is chosen based on the size of the image container, the amount of data needed and obtain immunity embedded characters [8].After filling the container is passed to the channel with the additive white Gaussian noise. A mixture of digital images, embedded characters and additive noise is fed to the receiver; in the emergency unit original empty container can be known and unknown. After the block, the result of transforming the character allocation algorithm with two digital correlated and solver, which performs the function of determining the value of the symbol of the transmitted information. For the operation of the system in sync generators PSP on the receiver and transmitter, the current system of generators, CAP, implemented in shift linear feedback register. Thus, synchronization is accomplished by specifying the initial state of the generator with other channels, were transferred to the keys, implemented model has the ability to modify the following parameters: the number of characters in the container (speed, which is measured in the number of bits per pixel images [9-10].The amplitude of the embedded symbol and noise in the channel ' degree polynomials, which form the pseudo-random sequence to replace of characters; and the type and parameters of the used algorithms of embedded symbols.

III. ALGORITHMS FOR EMBEDED CHARACTERS

To improve the transmission of basic information about the invisibility of integration is carried out only in the blue channel, how the human visual system is less sensitive to blue light. [1] let p = x, y) coordinates of the pixel in the image container to which implementation, (b) (p)-blue channel, intensity value of the container the image at the current position of p, si-current of the q-bit constant that determines the energy of bits. Then the modified value blue channel intensity: [11-12].

$$b`(p) = \begin{cases} b(p) + q, : s_i = 1 \\ b(p) - q, : s_i = 0 \end{cases} \quad (1)$$

After passing thenoisy channel, thevalue obtainedintensityof blue color channelwill bedistorted:

$$b``(p) = b`(p) + n(p) \quad (2)$$

Extractionof information transmittedbythe receiverfor known values ofb (p),that is,you have the originalcontainerunfilledat the receiver.Getting the value ofthe transmittedbits($s_i`$)bythe following:

$$s_i` = \begin{cases} 1, b``(p) - b(p) > 0 \\ 0, b``(p) - b(p) < 0 \end{cases} \quad (3)$$

A distinctive featureof this typeof algorithmsis the useof coefficientsto embeddiscrete cosinetransform (DCT)direct conversion ofselectedcoefficientsfor additiveembeddinginformation.

To reduce thevisibility of embeddinginformation is usuallyonly onefactor.Next isthe reverse.This approachhas the obviousdrawback, thereduction ofthe embeddedinformation [13].When comparingdifferent algorithmshiddeninformation, forfeatures are considered.For example,at the level ofintegrationof the coefficientsof the discretecosine transform(DCT) due to the use ofafactorof 64reduces the maximumamount of dataup to 64 times. Note that thelength of theCAP(Lpsp)variesfor differentalgorithms(X_{MAX}, Y_{MAX} -sizeimages):

•concealmentalgorithmatthe image space:

$$L_{psp} = \frac{X_{MAX} \times Y_{MAX}}{N_{bits}} \quad (4)$$

WhereL_{psp} -lengthCAPNbits -the number oftransmitted information in bits.

•Concealmentalgorithmatthe spaceconversion factors:

$$L_{psp} = \frac{\frac{X_{MAX} \times Y_{MAX}}{N_{bits}}}{T_P} \quad (5)$$

WhereT_p -conversion option

ForDCTtransformation parameteris 64 insertion ofasingle factorof 64.

Studyinvisibilityfactembedsuseful information.To justify theuse ofbandwidthfor embeddinginformationinto digital imagesin Fig.3shows theinsertionof a regular sequencewithout the use ofbandwidth andusingPSP (length120) forinformation hidingalgorithmon the levelof image spacewhen used as acontainerof digital photography.

Figure.3: shows theoriginal photo.

Fig.4the original photoshowsthe completedcontainer forembeddinginformation in thecase ofa photowithout usingbandwidthatq =50.

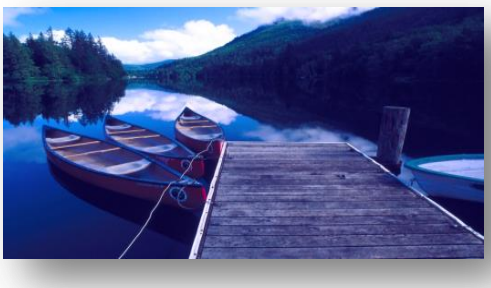

Figure.4: Filled containerembeddinginformationinto the picture without using (p_{ap}, q = 50).

IV. DISCUSSION AND RESULT

The analysis shows that the use of memory bandwidth can increase your steal Th fact embedding, since the transfer of the regular sequence, without the use of bandwidth, leads to a change in color of the image. Distortion caused by embedding with lid, as adding noise in the image. Criteria for assessing the degree of difference between containers offered for peer review:

a) The lack of distortion.
b) Distortion of individual pixels.
c) A small distortion of the individual fragments.
d) Strong distortion of the individual fragments.
e) Strong distortion of the image.

We have combined the pseudo supplements and methods for identifying the dominant pixels; we proposed to extract an image from the color of the s CSE.

(Fig. 5) shows the value of the initial margin of certain criteria. Therefore, when you set the criteria for an inconspicuous embedding for the red channel of the maximum amplitude of embedding (q) corresponds to 28 shades of color components for green shades-15 shades of color components, 53-blue component of the color. Results are consistent with the theoretical data, according to which the sensitivity of the human eye to little blue channel and integration must be performed precisely in the blue channel of the image. Maximum amplitudeembedding increases for the red channel-59 shades of color components for the 41 shades of green color components, blue-88 shades of color components.

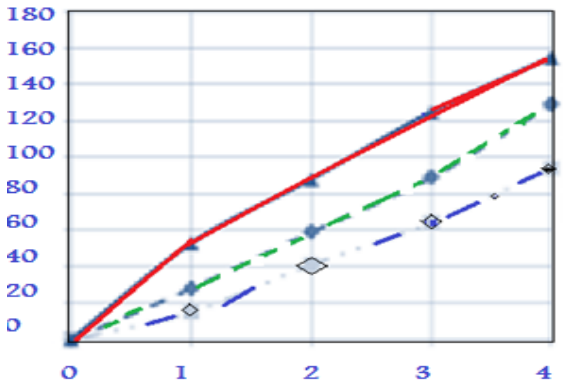

Figure.5: embedsthe space levelimages.

In considering thework of algorithmsembeddedinformation at theDCT coefficients(Figure 6)are similar tothe resultsobtained above.Integration into thebluechannelshows the bestresults in terms ofstealthfactembedded.

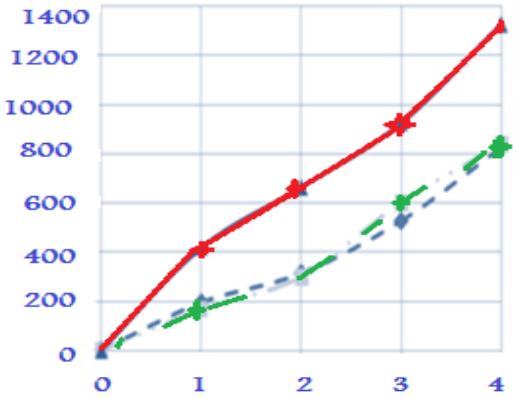

Figure.6: Peer review for the algorithm embedded at the DCT coefficients.

Each algorithm shows that the maximum amplitude of the building will be built to a minimum and maximum image area. Thus, providing for maximum stealth fact insert a fixed energy is required to use the built-in bit integration factors.

The standard measure of the differences between the two images I1 and I2, dimension M × N, is a measure of the ratio of signal to noise ratio (PSNR peak signal-to-noise ratio:

$$PSNR(I_1, I_2) = 10 \cdot log_{10}\left[\frac{M^*}{MSE(I_1,I_2)}\right] \quad (6)$$

M * -the maximumvalue of the normof differencesbetween pixels

$$\|I(k,1)\|\left(\|I_1(k,1) - I_2(k,1)\| = |I_2(k,1)|^2\right) \quad (7)$$

$$M^* = max\|I(k,l)\| = max|I(k,l)|^2 \quad (8)$$

MSE (I_1, I_2) mean square erroris defined as follows:

$$MSE(I_1, I_2) = \frac{1}{M \cdot N}\sum_{k=0}^{M-1}\sum_{l=0}^{N-1}\|I_1(k,l) - I_2(k,l)\| \quad (9)$$

$$MSE(I_1, I_2) = \frac{1}{M \cdot N}\sum_{k=0}^{M-1}\sum_{l=0}^{N-1}|I_1(k,l) - I_2(k,l)|^2 \quad (10)$$

For installationin a singlecolor channel, allvalues of the othercolor channelsof source andfill the containercompletely identical to the case of 8bitsperpixel valueM * =255 ×255 =65,025. In Fig.7shows a plotof the amplitude ofPSNRembeddingalgorithmsforinformation hidingat theimage spaceandthe space levelDCT coefficients.

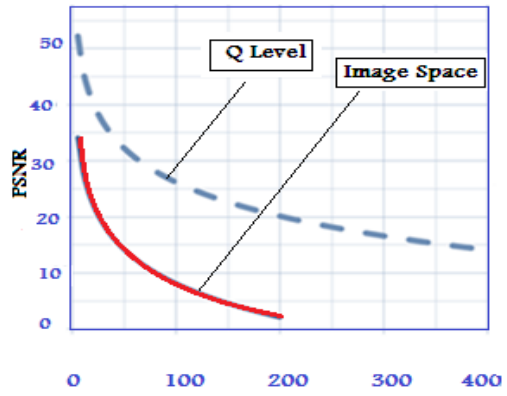

Figure.7: shows a plot of the amplitude of PSNR

V. CONCLUSIONS & RECOMMENDATIONS

An analysis of the numbers so that when the difference of fixed amplitude implement peak signal-to-noise ratio is 18 DB. The PSNR for fixed ratios can be used to order the superior value of the amplitude compared to insert images of space. The results of this analysis correspond to peer review. Admission is 10-2; ratio of embedded bits of noise in the channel 16.5 DB): implementation of image space-0.0033 bit/p the space factors 0.0033 bps, necessary in the future, noise, we learn that it's easy for independent Gaussian noise. We hope to see a more complete image Watermarking methods and better improvement in the near future, additional image detection methods for filtering images. The proposed test method for a standard set of CMU/MIT test exceeds all known methods in speed and quality of detection.

REFERENCES

[1] Janakiraman T. N., and Chandra Mouli P. V. S. S. R., " Color Image Edge Detection using Pseudo-Complement and Matrix Operations", Proceedings of World Academy of Science, Engineering and Technology Volume 32, ISSN 2070-3740, 2008.

[2] Ingemar, J. Cox. Digita l waterma king and d ste gano graphy J. Ingemar Cox, L. Mi ller Matt er Matt hew, A. Bloom Jeffrey effrey [et al.]. – Mor gan Kaufmann Pu blis hers, 2008.

[3] Van de Weijer J.; Gevers Th. and Geusebroek J.M., " Color Edge Detection by Photometric Quasi-

[4] Invariants", Proceedings of the Ninth IEEE International Conference on Computer Vision (ICCV 2003) 2-Volume Set, 2003.

[5] F. Bartolini, M. Barni, and A. Piva, "Performance analysis of ST-DM,watermarking in presence of nonadditive attacks", IEEE Transactions onSignal Processing, Vol. 52, No. 10, October 2004, pp. 2965–2974.

[6] B. Chen and G. Wornell, "Quantization index modulation: a classof provably good methods for digital watermarking and information embedding", IEEE Transactions on Information Theory, Vol. 47, No. 4,May 2001, pp. 1423–1443.

[7] M. Barni, F. Bartolini, A. De Rosa, and A. Piva, "Capacity of full frameDCT image watermarks", IEEE Transactions on Image Processing, Vol.9, No. 8, August 2000, pp. 1450–1455.

[8] K. Su, D. Kundur, and D. Hatzinakos, "Statistical invisibility forcollusion-resistant digital video watermarking", IEEE Transactions onMultimedia, Vol. 7,No. 1, Feburary 2005, pp. 43–51.

[9] Mei-Yi, W., Yu-Kun, H, Jia-Hong, L. (2004): An Iterative Method of Palette Based mage Steganography, Journal of Patern ecognition Letters, Vol(25).

[10] Xiang-yang, L. , Dao-shun,W., Ping, W., Fen-lin, L.((2008): A review on Blind

[11] Detection for Image Steganography, Journal of Signal Processing, Vol (88), Issue (9).

[12] Pei-Chun Chen, Yung-Sheng Chen,A communication system model for digital image watermarking problems, IAENG Computer Science, 34:2, IJCS_34_2_01 http://www.iaeng.org/IJCS/issues_v34/issue_2/IJCS_34_2_01.pdf

[13] http://vis.uky.edu/~cheung/courses/ee639_fall04/readings/watermarkITsurvey.pdf

[14] http://www.springer.com/978-3-642-14312-0

[15] http://www.hindawi.com/journals/ijvt/2012/50625/

Takialddin Alsmadi is working at Department of Communications and Electronics Engineering.
College of Engineering, Jerash University, Jerash-Jordan, He received his PhD in engineering (System analysis, control technology and Information processing) His research areas of specialization are differential pulse to code modulator and demodulator, computer science and technology, information system, digital processing design and analysis.

Mohammed Miata is working at the Computer Science Department, *King Saud University*, *Riyadh*, *KSA.*

How to cite this paper: Takialddin A. Al Smadi, Mohammed Maitah,"An Efficiency and Algorithm Detection for Stenography in Digital Symbols",IJCNIS, vol.6, no.1, pp.34-38,2014. DOI: 10.5815/ijcnis.2014.01.05

