Tikrit Journal of Pure Science
ISSN: 1813 – 1662 (Print) --- E-ISSN: 2415 – 1726 (Online)
Journal Homepage: http://tjps.tu.edu.iq/index.php/j

steganography in colored images based on biometrics

Zeena Nabeel Jameel AL-Kateeb , Marriam Raad Jasim Mohammed AL-Bazaz
Department of Computer Science, College of computer science and Maths., University of Mosul. Mosul, Iraq
DOI: http://dx.doi.org/10.25130/tjps.24.2019.056

ARTICLE INFO.
Article history:
-Received: 2 / 4 / 2018
-Accepted: 20 / 5 / 2018
-Available online: / / 2019
Keywords: steganography, biometrics,hand geometry
Corresponding Author:
Name: Zeina Nabeel Jameel
E-mail:
zeenaalkateeb@yahoo.com
Tel:

ABSTRACT

Due to the great significance of the concealment and transfer of confidential data and the many and varied algorithms presented in this field, as well as the big and rapid development of the use of biometrics in the issues of reliability and verification of the identity of people in support of information security. Therefore this research has provided a suggested algorithm to hide confidential data in colorful images based on the features of engineering dimensions of the human hand as one of the types of biometrics; we extracted a set of these characteristics and processed them to build a matrix that specifies the map of the distribution of confidential data in the cover image. The proposed method was applied to a set of images to hide a set of confidential messages and the visual quality of the cover image was not affected after the concealment. The practical results explain the efficiency of this method was measured in terms of comparison between the original image before and after concealment. The performance of the algorithm and the method of its application were measured using measures of efficiency of the work, whereas the Peak Signal Noise Ratio was used, the highest ratio obtained was 81.3417, and Mean Square Error was approximately 0.0008 as a maximum limit, while the error rate was the restored confidential message after hiding Bit Error Rate = 0 in all cases.

1. Introduction

Owning to the tremendous development in the field of information security technology and methods of data transfer, the issue of transferring a confidential message in an insecure network has become a very important subject and the algorithms and special methods of providing security for communications are growing and developing greatly because of their importance in human life especially after the spread of e-government in most countries of the world. In general, technologies to improve the security of information security technology can be divided into two main techniques: information encryption and information concealment.

In encryption technique, the content of the confidential message is changed in such a way as to ensure that no third party can read the confidential message correctly. In the technique of hiding information, the confidential message is hidden in such a way as to ensure that no third party can detect the existence of the confidential message itself which considers integrated technical concealment technology for encryption technology [1] [2]

Biometrics is one of the fastest growing branches of information security technology. Biometrics can be defined as automatic methods and means of identification the identity or recognize it based on the biological and behavioral characteristics of the individual. There are many advantages to biometric techniques when used in different fields that give them priority and greater quality compared to traditional methods. Therefore, many countries have been using credential systems on biometrics to take adequate measures against increasing security risks in the modern world. In this research we have adopted one of the types of biometrics, which is the measurement of engineering dimensions of the human hand to hide confidential data in the form of a kind of information security technology, where the cover image can be transferred and carrying confidential data to ensure safe arrival from sender to recipient and then opened by the recipient and

obtained Confidential data with accuracy and clarity[3].

2. Biometric

There are many biometrics. The effectiveness of biometrics varies depending on the time and place of use and their usage rates vary, the strengths and weaknesses of each system must be determined before selecting which one will be used in a particular application depending on the suitability of that application according to the availability of requirements and capabilities. There are several factors to notice and consider when choosing the appropriate system for an application. [4] Biometrics can generally be classified into two main categories:

Physiological biometrics, these parameters are defined as distinctive traits as it is unique to each person from the rest of his peers and this type of biometrics called static measurements name as it depends on the extraction of data from the anatomical measurements of the person, such as Fingerprint, Hand geometry, Retina, Iris Face Recognition, [6] [5], Behavioral biometrics are defined as behavioral characteristics of each human being who are different from others whereas this type of biometric is less stable than the first type. The behavioral characteristics of the individual may be influenced by factors such as stress, weakness, illness or age, These features are characterized by less secure, such as digital signature, voice recognition, fingerprint on keyboard [7, 6, 5] Key Stroke.

The measurement of the geometric dimensions of the human hand "Hand geometry" is one of the physiological Biometric which is based on the reliability of the people depending on this measure according to the reality that almost everyone has a unique hand geometry unique to the rest of the people are not much affected by the factors of time and aging, as there are reliable measurements and engineering features as well as reference points can be identified and adopted for the geometric extraction of each human hand, including the length and width of the fingers and the length and width of the palm and in addition to the measurements of corners confined between some points there are several merits and features of the use of engineering dimensions of the human hand, the most important ease of use, the possibility of using cameras with low resolution accuracy, saving the low cost and use of a small storage space in addition to the fact that this technology is unobtrusive for users and High acceptability [10] [9] [8].

3. Hide in photos

Steganography originates from the Greek word Steganos, which literally means cover writing.

Steganography can be defined as a technique of hiding confidential data within other data, so that no unauthorized person can detect the existence of confidential data, which ensures that it is safe from the sender's use to the recipient. Nowadays, covered writing systems can use different types of media as a cover for transmitting confidential data since it is possible to use audio, video, images, and communications in addition to other methods and techniques [11] [12].

Due to the availability of digital images the large number of transmission has been used as a medium, and color images provide the possibility to hide more data than gives the user greater freedom of hidden data size hidden

4 . Previous works

The idea of research is based on two types of research: a type that works to create a non-sequential mechanism to hide data and the other type depends on the uses of biometrics in reliability systems and hide them in Steganography methods. Most previous works of the first type have hidden a particular text or image based on chaotic systems to generate random chains determine the map of the spread of secret data was used. [11] Lawrence's famous triad system was used to generate three matrices, two of which were used to determine the distribution map of hidden data.

The paper [12] proposed a method for encrypting confidential data based on an anarchic system and then hiding it using the 3-3-2 LSB method of concealment. The research [13] provided a new and effective approach to masking the image based on individual value fragmentation (SVD) on each component of colorful image components where the compressed image coefficients are obtained and a key is used to rearrange these factors by using the chaotic function.

While the paper [14] was directed to the use of DNA which is one of the types of biometrics to hide the data. The research proposed design of a system that works to encrypt the data using the RSA algorithm and then hide it in the DNA series using a secret key that is the seed of a random number generator.

5. Suggested algorithm

The proposed algorithm can be divided into two main phases:

The phase of concealment of confidential data where the sender of the confidential message to carry out all the steps of this stage to get after completing all the steps on the image carries a secret text message scattered in a non-sequential manner, ensuring that the message cannot be obtained by unauthorized people to read. Receiving the message by the authorized person, it takes the steps of this stage to complete the text of the confidential message. Figure (1) illustrates the algorithm's work method in a simplified figure.

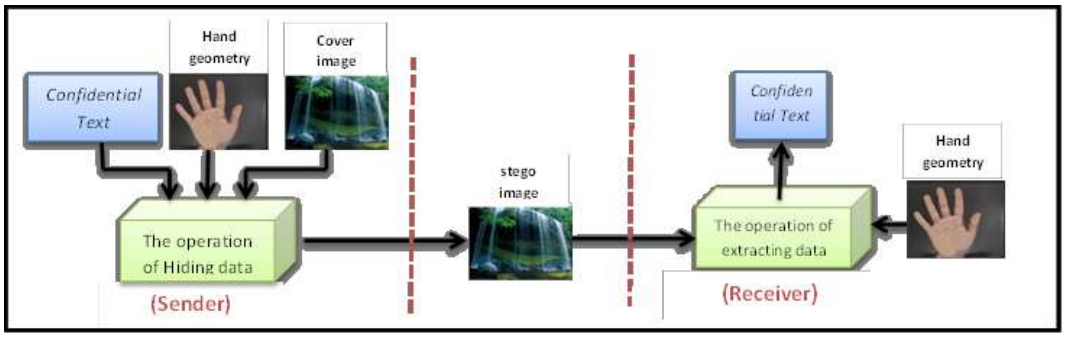


Figure (1): general structural of algorithm

6. Data masking phase

The first step (data entry): in which several elements are inserted

- A number representing the hand_no hand code, which will depend on its geometric properties in the identification of the concealment map, which is an integer number from 1-10, where 10 images belonging to 10 people are located at both of the sent and received communication.
- Human hand image which will adopt their hand_image features.
- Cover image.
- Secret text that wanted to hide.

The second step (extraction of properties): At this stage,one deduce fifty properties of the dimensions of the engineering dimensions of the human hand from the length of the palm and its width in addition to the lengths of the fingers, and more than the width of each finger, in addition to some angles and spaces and linear sections, and Table (1) shows the 50 properties that were used in the proposed algorithm in detail. It should be noted that the properties of engineering dimensions of the human hand are stored as a one-dimensional matrix features (50), whose data are real values.

Table (1) 50 properties adopted in the proposed algorithm

Property	Number
Finger length for each of the following fingers (pinkie, finger ring, finger ring, middle, index finger, and thumb).	5
The first width of the fingers, which represents the end of the finger far from the center of the body for each of the following fingers (pinkie, finger ring, finger ring, middle, index finger, thumb).	5
The second width of the fingers, which represents the width of the middle of the finger almost to each of the following fingers (pinkie, finger ring, finger ring, middle, index finger, thumb).	5
The third width of the fingers, which represents the end of the finger close to the center of the body for each of the following fingers (pinkie, finger ring, finger ring, middle, index finger, thumb).	5
Palm width in two areas.	2
Length of palm and indicated to.	1
Diameter the small axis of the oval area that forms the tip of the finger for each of the following fingers (pinkie, finger ring, finger ring, middle, index finger, and thumb).	5
Diameter the large axis of the oval area that forms the tip of the finger for each of the following fingers (pinkie, finger ring, finger ring, middle finger, and thumb).	5
The area of the oval area that forms the tip of the finger for each of the following fingers (pinkie, finger ring, finger ring, middle finger, thumb).	5
Written and referenced sections.	4
The angles are enclosed between written sections.	8
Total properties.	50

The third step (processing): in which the text to hide secret_text is processed by converting it to the ASCII code that represents each character, then converting the output to the binary format, and Figure 2 shows the procedure. The size of the hidden text sizeof _secret_text is also calculated.

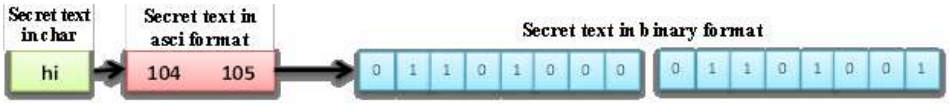


Figure (2): shows the conversion of the secret text into binary forma

A matrix is also created to represent the hid_pos distribution map based on the 50 properties extracted from the human hand image, where hid_pos is a matrix whose elements are integer correct values

ranging in value from 1 < hid_pos <(M * N) Thus, we have a single-dimensional matrix with a set of elements. We can hide a secret text message with a size of 1 (M * N). When creating a hid_pos array, hide the supported image encoding code and the size of the secret text.

Step 4 (Hide Data): At this stage, all of the following are hidden:

- Human hand image coding code whose characteristics will depend on the mapping of the hand_no mask.
- Size of hidden text sizeof _secret_text
- secret_text.

The encoding of the approved human hand image encoding and the size of the hidden text at a specified location of the image is by agreement between the sender and the recipient. The text is hidden using the 3-3-2 LSB method so that a full character of the secret text is hidden in each bitmap cell of the raster cells of the cover image. The first three bits of the letter are hidden in the red chip of the raster cell. The next three bits are hidden in the slide And the last two characters of the letter are hidden in the blue segment of the raster cell, which allows to hide relatively large size text compared to the traditional LSB mask and Figure 3 shows the mechanism of concealment. Flowchart (1) shows the stage of data concealment that occurs when the person sending the message.

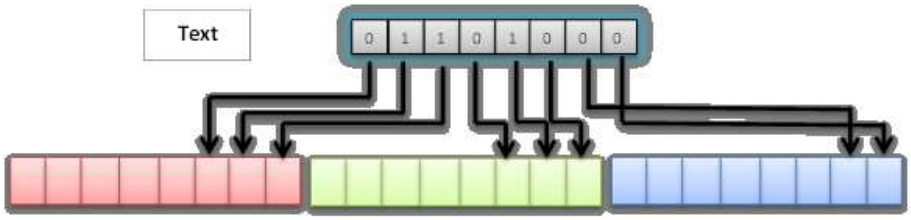
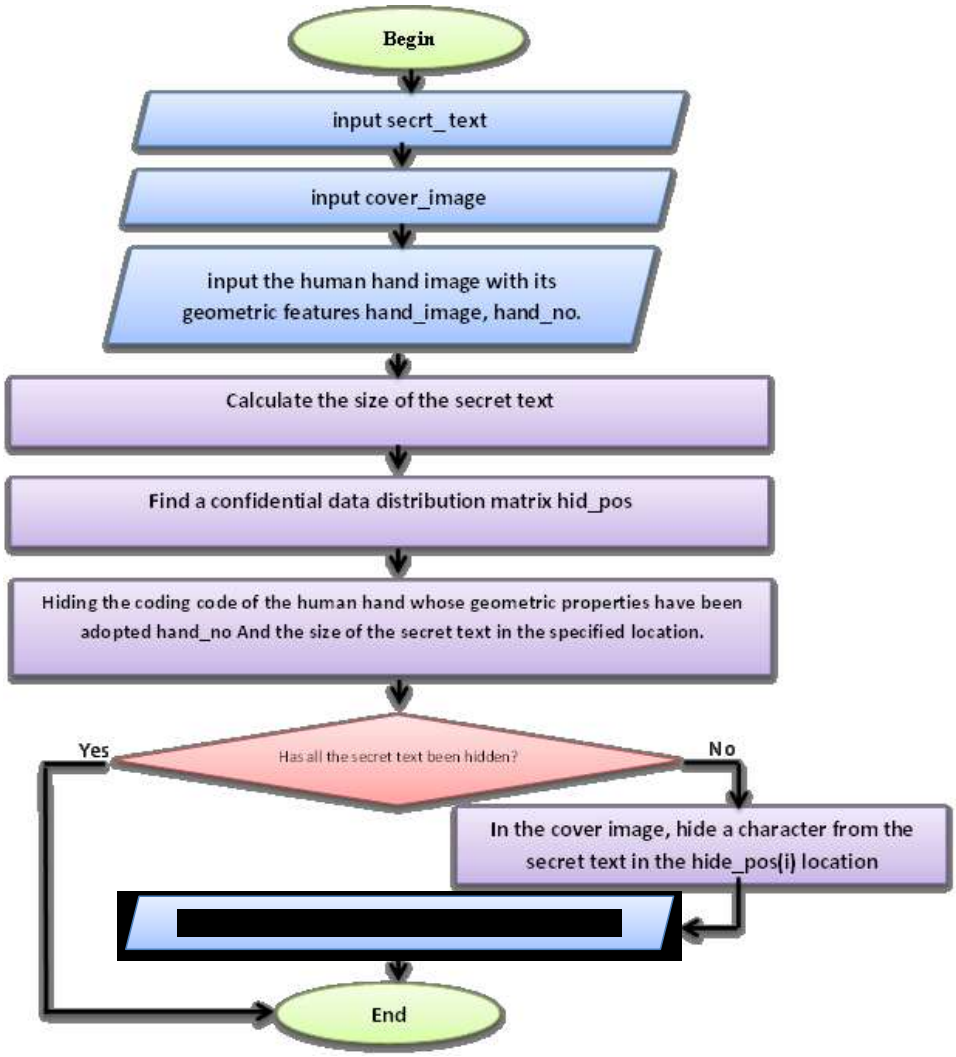


Figure (3): Mechanism of data concealment in a 3-3-2 LSB format

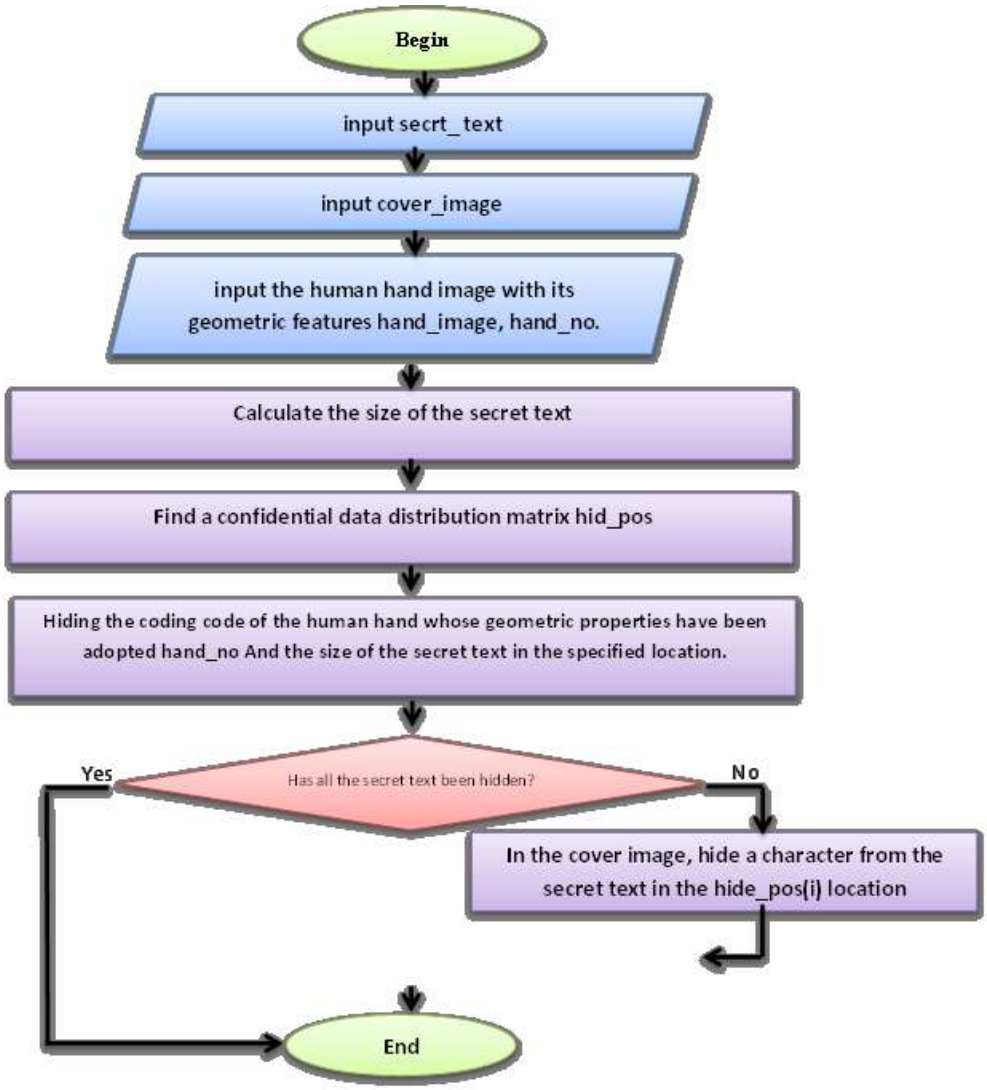


Flowchart (1) process of hiding the secret text

The first step (data extraction): After receiving the image that hides the confidential message, the code of the hand_no human hand image coding is first extracted. Whose properties were adopted in the masking phase of the custom site in the cover image, and extracts the size of the hidden text sizeof _ secret _ text. Then enter the selected image in order to extract the characteristics of its engineering dimensions hand_image.

The second step is (to build the map of the secret data distribution). Once the image of the hand is adopted, the properties are extracted to obtain the characteristics matrix. The data distribution matrix is then constructed in the same manner as the third step of the data hiding phase

Step 3 (Extracting the Secret Text): From each location in the data distribution matrix, a full byte of data is extracted the data extracted from its binary form is then converted to a letter format to give the text of the confidential message. The flowchart shows the steps to extract the secret text from the cover image**.**



7. Quality measures of hidding

In order to prove the quality of the proposed algorithm, the following measures were applied to measure the quality of concealment and data retrieval efficiency:

Mean Sequare Error (MSE)

It is calculated from the following law

MSE=1/((M*N)) ∑_(i=1)^n▒∑_(j=1)^n▒〖(C(i,j〗)-S(i,j))^2

Where C is the image cover, as S is the picture that contains the secret text

Peak Signal to Noise Ratio (PSNR)

This measurement is based on the peak-to-noise ratio, which is good at maintaining the edges and angles, depending on the following law

MSE〗] (in /2]PSNR=10 〖 log〗 _(10) [C max (dp

Note that Cmax is the highest color value in the image.

Bit Error Rate(BER):

This metric is used to determine whether the text has been fully retrieved knowing the number of bits retrieved using the following code

BER=(no. of wrong bit/(no.) of original bit)*100

8. Results and discussion

The proposed algorithm was applied to a set of images of different sizes,the proposed algorithm was applied to a set of images of different sizes where a 100-character text massage was hidden, and the results obtained were as shown in table (2), which illustrates the use of the algorithm in detail where adopted to take pictures of different sizes and standards were applied to measure the quality of concealment and data retrieval efficiency was measured as the peak signal to noise ratio and error rate in a serrect message after hiding.

Table (2) shows the results obtained from applying the proposed algorithm

No.	Original Image	Image size	MSER	MSEG	MSEB	PSNR	BER
1	hid1.png	531 * 852	0.0008	0.0008	0.0001	77.5737	0
2	hid2.png	582 * 777	0.0007	0.0007	0.0001	78.0693	0
3	hid3.jpg	522 * 870	0.0005	0.0007	0.0001	78.0940	0
04	hid4.jpg	582 * 777	0.0001	0.0001	0.0000	76.6862	0
5	hid5.png	603 * 753	0.0007	0.0008	0.0001	77.7882	0
6	hid6.png	672 * 1200	0.0004	0.0002	0.0001	81.3417	0
7	hid7.png	804 * 1004	0.0003	0.0004	0.0001	80.0212	0
8	hid8.jpg	708 * 1136	0.0005	0.0004	0.0000	80.3186	0
9	hid9.jpg	672 * 1200	0.0004	0.0004	0.0001	80.4846	0
10	hid10.jpg	708 * 1136	0.0004	0.0003	0.0001	80.7373	0

Experience showed the quality of the algorithm used, as the process of data concealment did not affect image quality. Data extracted after the decoupling were not changed or lost, thus supporting the proposed algorithm**.**

9. Conclusions and Future Actions

The use of hidden data technology in digital images based on geometrical dimensions integrates the concealment features with the biometrics features, which supports concealment and provides the ability to prevent hackers from penetrating confidential data. The use of the proposed algorithm provides high storage capacity with good hiding efficiency, The concealment is not noticeable to the human eye. The algorithm can be applied to hide in audio, video or any type of multimedia as well as the possibility of replacing the geometry dimension with any other type of biometrics.

References

[1] Nilizadeh A. , Mazurczyk W. , Zou C. ; Leavens G. T.,(2017) “Information Hiding in RGB Images Using an Improved Matrix Pattern Approach”, produec Conference: 21-26 July 2017, IEEE.

[2] Katre B.,Bhrati ,(2017),“Dynamic Key based LSB Technique for Steganography”, International Journal of Computer Applications (0975 – 8887) Volume 167 – No.13, June 2017

[3] Hasso Maha, Al-kateeb Zeena N.,(2013), “ Building a system to identify people based on the human hand geometry”, AL-Rafidain Journal of Computer Sciences and Mathematics , Volume 10-Issue: 1 ,Pages 47-60

[4] Batra N., Kaushik P., (2012), "Implementation of Modified 16×16 Quantization Table Steganography on Colour Images", International Journal of Advanced Research in Computer Science and Software Engineering ,Volume 2, Issue 10,PP.(244-250) .

[5] Caldera-Serrano, Jorge (2008), “Changes in the management of information in audio-visual archives following digitization: Current and future outlook”, Journal of Librarianship and Information Science, 40 (1).- pp.(13- 20).

[6] Deb S., (2004), "Multimedia Systemsand Content-Based Image Retrival", Idea Grop Inc. (IGI).

[7] Giesing, Ilse (Compiler), (2003), “Biometrics”, University of Pretoria.- pp. (49-76).

[8] Ríha Zdenek and Matyáš Václav, (2000), “Biometric Authentication Systems”, FI MU Report Series, Masaryk University.

[9] Roberts Chris, (2006), “Biometric Technologies-Palm and Hand”, http://www.ccip.govt.nz/newsroom/information-notes/2006/biometricstechnologies- palmhand.pdf.

[10] Varchol Peter, Levický Dušan, (2007), “Using of Hand Geometry in Biometric Security Systems”, Radioengineering, VOL. 16, NO. 4, pp(82-87).

[11] Zhang J., Hou D., Ren H.,“Image Encryption Algorithm Based on Dynamic DNA Coding and Chen’s Hyperchaotic System”, Hindawi Publishing Corporation, Mathematical Problems in Engineering, Volume 2016, Article ID 6408741, 11 pages ,http://dx.doi.org/10.1155/2016/6408741.

[12] Bandyopadhyay D., Dasgupta K., Mandal J. K., Dutta P.,”(2014), a novel secure image steganography method based on chaos theory in spatial domain”, International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 3, No 1,.

[13] Rashied , M.M., (2016),“Image steganography by using SVD and chaotic Zig Zag map ”,Iraqi Journal of Information Technology, Volume: 7-Issue: 2, Pages: 45-56.

[14] Metras Ban, Abo Adeeba, (2013), “ information hiding in DNA sequence by using the secret key as seed for generating random numbers”, IRAOI JOURNAL OF STATISTICAL SCIENCES, Volume - 13 Issue: 25 , Pages 430-440

الاخفاء في الصور الملونة بالاعتماد على المقاييس الحيوية

زينة نبيل جميل الخطيب ، مريم رعد جاسم البزاز

قسم علوم الحاسوب ، كلية علوم الحاسوب والرياضيات ،جامعة الموصل ، الموصل، العراق

الملخص

نظرا للأهمية الكبيرة لمسالة اخفاء البيانات السرية ونقلها والخوارزميات الكثيرة والمتعددة التي قدمت في هذا المضمار بالإضافة الى التطور الكبير والسريع الحاصل في مجال استخدام المقاييس الحيوية في مسائل الوثوقية والتأكد من هوية الاشخاص دعما لأمن المعلومات. لذا فقد قدم هذا البحث خوارزمية مقترحة لإخفاء البيانات السرية في الصور الملونة بالاعتماد على خصائص الابعاد الهندسية لليد البشرية كأحد انواع المقاييس الحيوية، اذ قمنا باستخلاص مجموعة من تلك الخصائص ومعالجتها لبناء مصفوفة تحدد خريطة توزيع البيانات السرية في الصورة الغطاء. تم تطبيق الطريقة المقترحة على مجموعة من الصور لإخفاء مجموعة من الرسائل السرية وكانت الجودة البصرية للصورة الغطاء لا تتاثر بعد الاخفاء. النتائج العملية توضح فعالية هذه الطريقة من حيث المقارنة بين الصورة الاصلية قبل الاخفاء وبعده، كما تم قياس فعالية اداء الخوارزمية واسلوب تطبيقها باستخدام مقاييس لبيان كفاءة العمل، حيث تم استخدام مقياس نسبة ذروة الاشارة الى الضوضاء وكانت اعلى نسبة تم الحصول عليها هي 81.3417 ، كما كانت قيمة متوسط مربع الخطا تصل الى مايقارب 0.0008 كحد اعلى، في حين كانت نسبة الخطا في الرسالة السرية المسترجعة بعد الاخفاء تساوي صفر في جميع الحالات.