Digital Image Protection by Password

Mohamed Seidi Ahmed Hmadi[1] *and Salim Ali Salim Aloud*[2]

1- *Computer Science Department Faculty of Science Azzaytuna University,Tarhuna -Libya*
Hmadi2595@yahoo.com

2- *Computer Science Department Faculty of Science Azzaytuna University, Tarhuna -Libya*
salemali416@yahoo.com

Abstract:

The case of protecting literate property rights in digital images and digital data is very important because it protects the rights of individuals and institutions, especially data protecting, research and inventiveness. Among these data, digital data, specifically digital images and digital data have become prevalent in various processions of life and are circulated daily, whether on the mobile phone or the computer, which confirms the need to search for ways to protect ownership of any image that is circulating. In this study, a system was designed based on protecting any image using a password consisting of 6 characters. It is hidden inside the image and is considered invisible. When we need to prove the ownership of an image, the owner of the image, who is the owns password, is only the one who can prove its ownership by extracting the password from the digital images or digital data.

Key words : digital images, image rights, password extracting, password retrieving.

الملخص

تعتبر قضية حماية حقوق الملكية التي لها علاقة بالصور الرقمية والبيانات الرقمية مهمة للغاية لأنها تحمي حقوق الأفراد والمؤسسات ، وخاصة حماية البيانات والبحث والابتكار .ومنها البيانات الرقمية وتحديداً الصور الرقمية والتي تنتشر في مجالات الحياة المختلفة ويتم تداولها يومياً سواء على الهاتف المحمول أو الحاسوب ، مما يؤكد ضرورة البحث عن طرق لحماية ملكية أي صورة تنتشر .في هذه الورقة ، تم تصميم نظام يعتمد على حماية أي صورة باستخدام كلمة مرور تتكون من 6 أحرف، وهى مخفية داخل الصورة وغير مرئية الا لصاحب الملكية الفكرية (كلمة المرور) .عندما نحتاج إلى إثبات ملكية الصورة ، فإن صاحب الصورة ، يملك كلمة المرور الخاصة به ، وهو فقط الشخص الذي يمكنه إثبات ملكيتها عن طريق استخراج كلمة المرور من الصور الرقمية أو البيانات الرقمية.

من أهم مميزات هذا النظام أن لكل مستخدم بيانات محددة وموقع خاص به ، ويتم الحصول عليه من خلال تشفير كلمة المرور الخاصة به ، أي أن لكل مستخدم مفتاحه الخاص لحماية بياناته .بعد اختبار النظام أعطت نتائج ممتازة وفعالة حيث تم اختبارها على عدد كبير من الصور الرقمية وأظهرت كفاءة هذه النظام حيث وصلت إلى 100٪ حيث لم يستطع أحد فك أي صورة محمية بواسطة هذا النظام، بعد تجربتها ، حيث يمكن استخدام هذا النظام لحماية الصورة الرقمية على وسائل التواصل الاجتماعي ، وينم ذلك بوضع كلمة مرور عليها ، ويمتاز هذا النظام انه لا يغير في الصورة حيث يبقي على الصورة يان تكون عالية الدقة.

1. Introduction

In the current era, the era of communications and information technology, literate property rights have become one of the basics of work in various processions of life and all countries of the world. Embed robust and fragile watermark into the host image at the same time, so that the proposed scheme can possess dual functions: one is copyright protection, and the other is tampering detection. Their experiments to show the performance of the proposed scheme The enactment of laws that protect literate property rights, especially after the spread of electronic crime [2].

Designing and implementation of a digital watermarking system used for the copyright protection of digital images. This watermarking system involves both the visible and invisible watermarking or bitmap images. In the instance where invisible watermarking takes place, it is important to maintain the integrity or image quality of the image being watermarked [3].

To protect digital images or digital data, whether it is digital audio, image, or video. Digital materials have spread in all processions of life, especially after the spread of mobile phones with a digital camera, as millions of digital images are captured every moment around the world. Implements a self-embedding of TL bits and mapped embedding of SR bits and for that, block mapping is performed. The encrypted combination of both the codes (TL of parent block + SR of mapped block) is inserted in the 1st and 2nd least significant bits of the parent block. Encryption of watermark bits (unique for each watermarked image) helps it to sustain the block based attacks (vector quantization, collage and four scanning attack) [6]. Through various media, a very large number of digital pictures are exchanged without the permission of the owner of the image. For example, we find a journalist who risked his life in places of conflicts and wars to take a picture of the battles, and this image is considered his property and no one may reuse it except with his permission, since when this image is stolen, that he will in a position to prove he the owner of this image. Dealing with civilian journalists; the case of war correspondents accredited to the armed forces, as provided for in Article 13 of the 1907 Hague Regulations and Article 4(A)(4) of the 1949 Geneva Convention III, is only addressed incidentally [9].

2. literal review

Our goal is to provide a secure system that protects the literate property rights of the digital image. They insert the watermark in the frequency domain using discrete cosine transform. The choice of the positions of the watermark bits depends on a preprocessing study on the original and compressed–decompressed image [1].

As mentioned in [8], the constructing of the default JPEG code for the reordered coefficient sequence begins with the computation of the difference between the current DC coefficient and that of the previously encoded subimage.

In return we design a system will be available to everyone and anyone, leading and use it in an easy and fast way, and it takes a few seconds to get the job done. While in our work the size of the encryption for the image does not increase its actual size, and it is also prohibited to encrypt the same digital document again.

3. Problem statements

Image encryption along with image stitching provides a double layer of protection to the image, to achieve security and privacy during the communication [4]. In our system we introduce a designed system for the owner of any digital image, which can protect his password consisting of 6 digits that are hidden inside the image without having any effect on the image, as the storage in the first cells of the byte from bit 0 to bit number 4. And when it is necessary to prove the ownership of the image, the system asks the user who owns the image to enter the first 4 digits of the password. If it is correct, the remainder of the password is extracted and compared with the correct number, and if there is an error, it gives an error message or gives another word other than the one kept by the owner of the image.

4. Digital images

In the digital image RGB type each pixel consists of three components Red, Green, and Blue and each one from these components represents a number that extends from 0 to 255.They had implements a blind detection algorithm. In order to counter rotation and cropping attacks, our scheme adopts Speeded-Up Robust Feature to locate invariant key points [1].

As mentioned in, the choice of the positions of the watermark bits depends on a preprocessing study on the original and compressed-decompressed image [5].

possible features for a content-fragile watermarking scheme to allow several postproduction modifications. The second approach is designed for high-security applications to detect each bit change and reconstruct the original audio by introducing an invertible audio watermarking concept. Based on the invertible audio scheme, we combine digital signature schemes and digital watermarking to provide a public verifiable data authentication and a reproduction of the original, protected with a secret key [7].

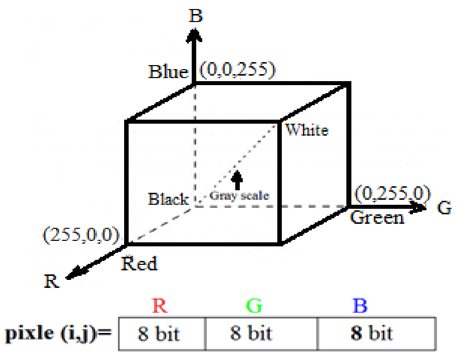


Figure (1) RGB type

The color red consists of 256 levels. Level (0) represents the color black and level (255) represents the color red and also green and blue. If the R = G = B then the color is gray. Leaving the idea of storing specific pixels, from which to start, to choose a consecutive 4-byte number, where the first four (0-3) digits of each byte are used to store data. The first stage includes uploading the image to be protected and then the system asks the user to enter a password consisting of 6 digits, then the protection order is:

1) The password is chosen from the first field from the left and it is encrypted by the algorithm to obtain the number 1, 2, or 3 to determine the location of the storage Red, Green, or Blue (RGB).

2) Column number 2 is encoded for grapes on the column number.

3) Row number 3 is encoded for grapes on the row number.

4) Field number 4 is encoded for the grains on the direction of data storage, where there are 8 directions, as shown in Figure (2).

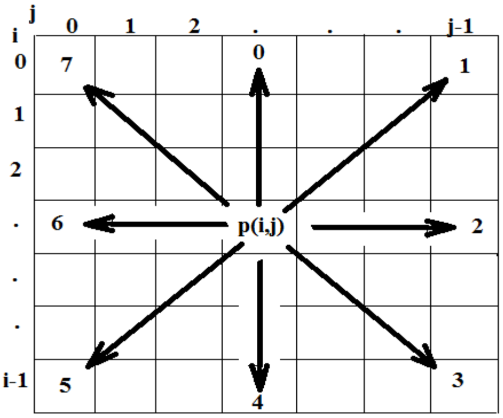


Figure (2) 8 directions

5) The two digits 5 and 6 represent the data that will be stored in the previously specified location, where each cell is divided into two parts, the first section of the 0 to 3 bits and stored in a number from 0 to 3 of the pixels. The second section of bits' number 4 to 7 is stored in bits' number 0 to 3 according to the specified direction. Where the first 4 digits are considered as the address constant in which you will deceive the data represented in digits 5 and 6 as in Figure (3).

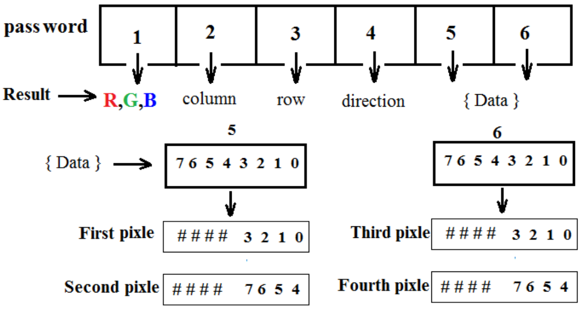


Figure (3) details of password

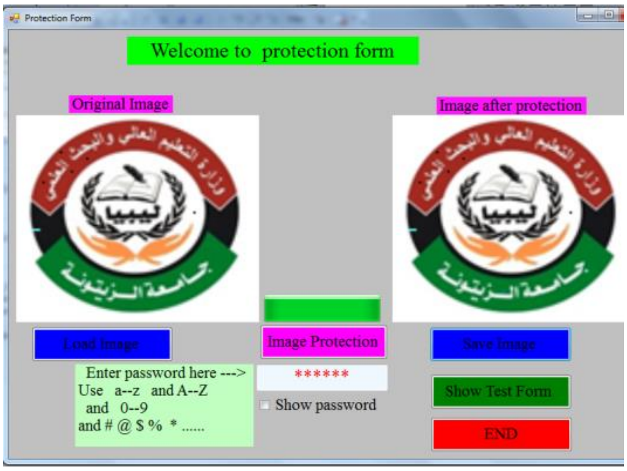
We also note that there are 4 levels of protecting, which are:

- The first level is to select the field Red or Green or Blue.
- The second level is to determine the column umber.
- The third level is to determine the row number.
- The fourth level is to determine direction.

So that if there is a level error, it will be difficult to access the specified location to see the stored data.

5. Test results

Figure (4.a, 5.a) image protection and Figure (4.b, 5.b) the image test by correct password Figure (4.c, 5.c) failed test because incorrect password.

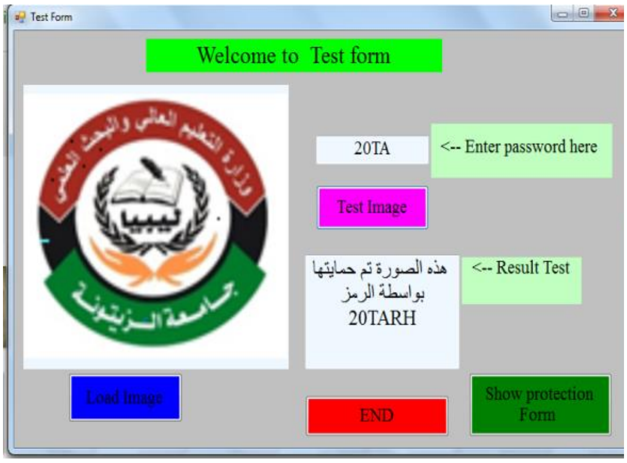


Enter password here --->
Use a--z and A--Z
and 0--9
and # @ $ % * ......

******

☐ Show password

Figure (4.a)

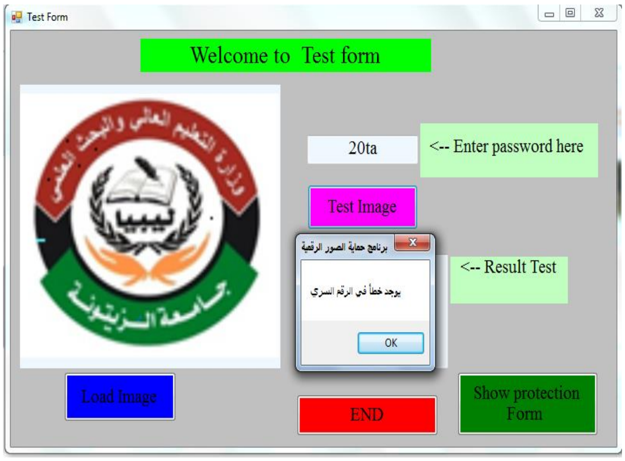


20TA <-- Enter password here

<-- Result Test

هذه الصورة تم حمايتها
بواسطة الرمز
20TARH

Figure (4.b)



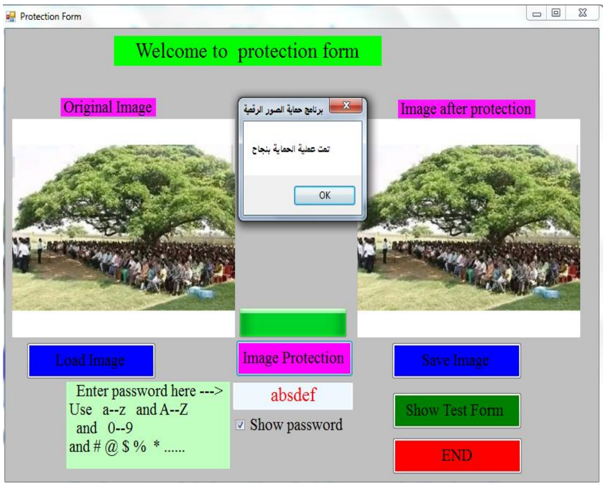
20ta <-- Enter password here

<-- Result Test

برنامج حماية الصور الرقمية

يوجد خطأ في الرقم السري

Figure (4.c)



برنامج حماية الصور الرقمية

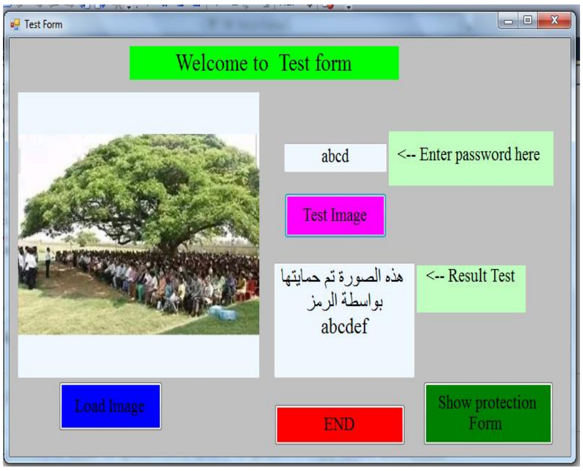
تمت عملية الحماية بنجاح

Enter password here --->
Use a--z and A--Z
and 0--9
and # @ $ % * ......

absdef

☑ Show password

Figure (5.a)

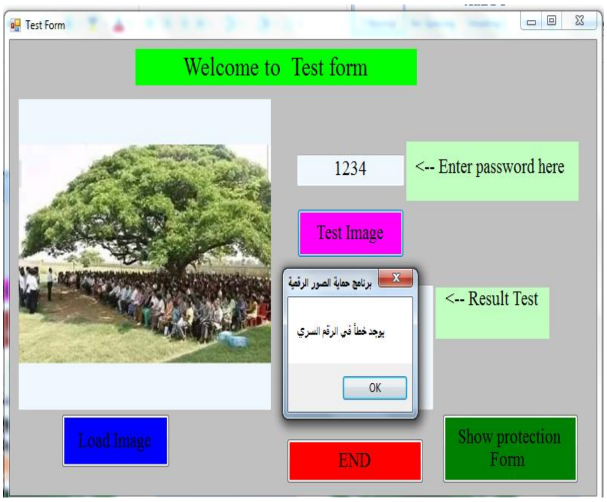


abcd <-- Enter password here

<-- Result Test

هذه الصورة تم حمايتها
بواسطة الرمز
abcdef

Figure (5.b)



1234 <-- Enter password here

<-- Result Test

برنامج حماية الصور الرقمية

يوجد خطأ في الرقم السري

Figure (5.c)

Note: The system is programmed using the visual code vb.net.

6. Conclusion

One of the most important features of this system is that each user has specific data and a specific location of his own, which is obtained by encrypting his password, meaning that each user has his own key to protect his data. After testing the system, it gave excellent and effective results, as it was tested on a large number of digital images from various and multi-use sources and showed the efficiency of this system, reaching 100% as no one was able to decode any image protected by this system, as in the figure some images System tested. Protecting a digital image on social media, is to place a password on them Also, if you never share high-resolution images, the opportunities are high that no one will be interested in stealing them. We can always make things official and register with this system as a copyright of owner.

7. Future works

This work has been achieved using very easy and simple algorithm, which does not consume time execution and less space of memory (one image per protection), next research area merging and protecting main while.

8. Bibliography

[1]Nesrine Tarhouni , Maha Charfeddine and Chokri Ben Amar " Novel and Robust Image Watermarking for Copyright Protecting and Integrity Control", Circuits, Systems, and Signal Processing (CSSP), 11th April 2020.

[2] Suhad A. Ali, Majid Jabbar Jawad and Mohammed Abdullah Naser, "Copyright Protecting for Digital Image by Watermarking Technique", Journal of Information Processing Systems Vol. 13, No. 3, pp. 599-617, Jun.2017.

[3] Ching-Sheng Hsu and Shu-Fen Tu, "Digital Watermarking Scheme for copyright protecting and tampering Detection ", International Journal on Information Technologies & Security, № 1 (vol. 11) pages (107-119), 2019.

[4] Jyoti T. G. Kankonkar and Nitesh Naik, "Image security using image encryption and image stitching", International Conference on Computing Methodologies and Communication (ICCMC), Conference Location: Erode, India, 2017.

[5] C.S. Hsu and S.F. Tu, “Digital watermarking scheme enhancing the robustness against cropping attack,” Proceedings of The 6th International Conference on Frontier Computing (FC2017), pp. 143-152, Osaka, Japan.

[6] I.A. Ansari, M. Pant, and C.W. Ahn, “SVD based fragile watermarking scheme for tamper localization and self-recovery,” International Journal of Machine Learning and Cybernetics 2015.

[7] Martin Steinebach and, Jana Dittmann, "Watermarking-Based Digital Audio Data Authentication ",EURASIP Journal on Applied Signal Processing 2003:10, 1001–1015, 2003 Hindawi Publishing Corporation, Retrieved 16/02/2021

[8] Rafael C. Gonzalez and Richard E. Woods" Digital Image Processing “Second Edition. Page 503, Prentice Hall 2002.

[9] I. Protection of Journalists and Media Professionals in Time of Armed Conflict, available at, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_rul_rule34. Retrieved 16/02/2021.