Journal of Computer Science 8 (1): 1-5, 2012
ISSN 1549-3636

Distribution Key in Eight Bit's Color Image Algorithm

Hamdi A. Al-Omari, Malek M. Al-Nawashi and Mohammed J. Bawaneh
Department of Information Technology, AL-Huson Polytechnic,
Al-Balqa Applied University, Jordan

Abstract: Problem statement: The networked multimedia systems have glorified the necessity for image copyright protection. To solve such problem an invisible structure called watermarking is added to an 8-bits color image in aim to mark it. The structure can be added by selecting bits under certain conditions; a few pixels of correspondence between the image and the ASSCI code. **Approach:** In this study, we employed a robust image-watermarking algorithm using the Key Distribution Algorithm to hide data inside 8-bits color image as a watermark. **Results:** Experimental results show that, Similarity in the embedding process making the selection bits from the image and did not make any change in the pixels, Entropy become equal zero where no changes in the existed pixels and the selected keys chosen from pixels which distributed in image, where does not exist any changed on cover image so any updating on image doesn't mean anything, so the key of the owner cannot be known. **Conclusion:** By applying Key Distribution algorithm the watermark can be extracted at low error rate.

Key words: Watermarking, steganography systems, key distribution algorithm, image-watermarking, networked multimedia, image algorithm, multimedia systems

INTRODUCTION

The growth of multimedia systems has caused relative problems to the protection of the rights of intellectual property which is true for images as a part of those systems. The types of protection systems involve the techniques of encryption that may represent text like numbers. Various invisible watermarking techniques were proposed such as the checksum which was used on image data, that it is incorporated in least significant bit. Another technique add s to pixel data the maximal length linear shift register in aim to identify the watermark through computing the correlation function of the sequence and the watermarked image (Holtz *et al*., 1996). The watermarking can implemented dependent on the visual channels of a specific image (Delaigle *et al*., 2002). IBM developed an exclusive visible watermarking in order to protect the images that a part of the digital Vatican library project (Cox *et al*., 2000; Wolfgang and Delp, 1996; Van Schyndel *et al*., 1994; Katzenbeisser and Petitcolas, 2002; Miller *et al*., 1999).

Distribution Key in 8bit Color Image Algorithm is one of the invisible watermarking methods (Van Schyndel *et al*., 1994; Trappe *et al*., 2001) that depends on selecting bits from 8bit image under certain conditions without any bit being changed to achieve pure hidden information was used to map between the ASCI code and the image using selected bits. The selected bits are inserted into eight levels binary tree in which the left is zero and the right is one as shown in Fig. 1.

To obtain the 256 branches each of them represents one character from the ASCI code (Trappe *et al*., 2001), such that each leaf node contains a pixel number which is selected from the image, so then numbers represent the secret key or signature of these characters.

Securing data transfer requires integrated techniques and procedures that provide high level of protection against the threats that may occur. Therefore, secure watermarking algorithm has become a very significant issue.

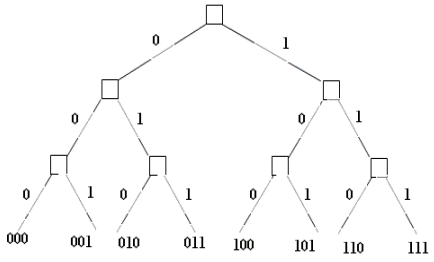

Fig. 1: Distribution key in binary tree

Corresponding Author: Hamdi A. Al-Omari, Department of Information Technology, AL-Huson Polytechnic, Al-Balqa Applied University, Jordan

MATERIALS AND METHODS

Many studies have been done on image watermarking security. Next is a brief description of some of these studies.

Isamil *et al*. (2010) show that that Zernike moments are the most widely used moments in image processing and pattern recognition and the computed Zernike moments in Cartesian coordinate are not accurate due to geometrical and numerical error. A robust image-watermarking algorithm using accurate Zernike moments. These moments are computed in polar coordinate, where both approximation and geometric errors are removed. Accurate Zernike moments are used in image watermarking and proved to be robust against different kind of geometric attacks. The performance of the proposed algorithm is evaluated using standard images. Results show that, accurate Zernike moments achieve higher degree of robustness than those approximated ones against rotation, scaling, flipping, JPEG compression and affine transformation and the embedded bits watermark can be extracted at low error rate.

Alshamasin *et al*., (2009) presented the gaussian noise and median filteras an approach capable of selecting the best blocks in the cover image for use in the watermarking process. Also , they propose a technique for robust digital watermarking system looking to find a relationship between the image contrast of the coverage and robustness of increasing the resistance of attacks.

Al-Hunaity *et al.* (2007) proposed a watermarking technique that deals with images in which the technique used to embed a watermark in the compressed wavelet Least Significant Bit (LSB) of pixels in the cover image in a specific pattern that will not be visible after coating and cause the cover image to become copyright by using the image of the watermark can be extracted later.

Liu *et al*. (2006) propose a watermarking scheme for digital image based on the Distributed Discrete Wavelet Transformation (DDWT) method with some modifications to improve its robustness. The scheme transforms original image data from the spatial domain into the frequency domain by using the DDWT technique and then embeds watermark information in the four sub bands in the frequency domain. In this way, we not only keep intact the salient feature of the DDWT method, which distributes hidden watermark information in the spatial coefficients and is robust against the cropping attack, but also greatly improve its performance so that the new scheme is robust against geometric attacks such as rotation or scaling and non-geometric attacks such as Gaussian noise, sharpening and contrast adjustment, too. Results show that the stego-image is superior and the watermark is robust against a variety of the geometric and non-geometric attacks mentioned above.

Ramesh and Shanmugam, (2011) proposed an image authentication system fragile tamper with the location in the wavelet domain. In this scheme, the secret data to be loaded is a logo. Watermark was generated by repeating the image of the logo so that the size of the watermark matches the size of the sub-band HH integer wavelet transform. To provide an extra level of security, the watermark is generated scrambled using a shared secret key. Integer wavelet transform was applied to obtain wavelet coefficients. Watermark was embedded in the coefficients with odd-even mapping. The experimental results showed that the proposed system detected and located at the pixel level alteration. Proposed scheme was tested with images of different sizes and falsification of different sizes. It has provided good results for the ranges of tampering from single pixel of a block of pixels. The watermark was done in wavelets; conventional attacks tattoo was not possible. The resolution of the location of sabotage was carried out at the pixel level. The quality of the watermarked image was always maintained while providing a pixel precision forging.

Yang *et al*. (2009) propose a visible watermarking scheme to satisfy the applications, in which the visible watermark is expected to combat copyright piracy but can be removed to losslessly recover the original image. They transparently reveal the watermark image by overlapping it on a user-specified region of the host image through adaptively adjusting the pixel values beneath the watermark, depending on the human visual system-based scaling factors. In order to achieve reversibility, a reconstruction/recovery packet, which is utilized to restore the watermarked area, is reversibly inserted into non-visibly-watermarked region. The packet is established according to the difference image between the original image and its approximation, version instead of its visibly watermarked version so as to alleviate its overhead. For the generation of the approximation, they develop a sample prediction technique that makers use of the unaltered neighboring pixels as auxiliary information. The recovery packet is uniquely encoded before hiding so that the original watermark pattern can be reconstructed based on the encoded packet.

Findik *et al*. (2010) propose a robust image watermarking technique using Support Vector Regression (SVR) and particle swarm optimization is introduced to protect intellectual property rights of the

gray images in discrete cosine transform domain against a variety of desynchronization attacks. After the division of the original image to 8×8 non-overlapping blocks, frequency coefficients of each block are found using discrete cosine transform. Positions if the inputs and output, among the low frequency coefficients which have the significant characteristics of the image, which are used to train SVR are obtained by using particle swarm optimization technique. After SVR is trained using to obtained positions of the inputs and output, watermark embedding and extracting processes are implemented using the trained SVR. Experiments implemented using the optimized coefficients selected among low frequency coefficients shoe that our watermarking technique has better watermark extracting success after the resynchronization attacks.

Aliwa *et al*. (2010), proposed a firm authentication method by using some features of the original name of the holder with the passport number and digest with passport's photo. The method hides invisible watermark which contains the digest name and passport number inside the passport's photo. The computer scanning process was used to check passport's photo has been not replaced by comparing the invisible watermark with the digest name of the holder and passport number.

Ramirez *et al*. (2004) propose an adaptive watermarking algorithm, in which the watermark is a binary image such as a logotype related directly to the image owner. Obviously the information amount of this type of watermark is much larger than the amount of a pseudorandom pattern generated by secret key. This fact makes it difficult to embed a bi-dimensional watermark code into a given image in an imperceptible way. To achieve this goal, they proposed an imperceptible adaptive embedding algorithm using the Just Noticeable Difference (JND) criterion. The evaluation results show the desirable features of proposed algorithm, such as the watermark imperceptibility and its robustness against attacks such as: JPEG compression, filtering and impulsive noise.

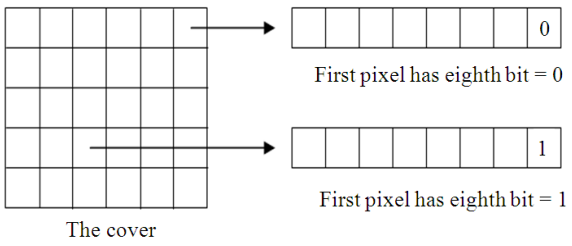

Fig. 2: Search to build first level in the tree

Proposed algorithm: Here we will discuss the methodology of algorithm through five steps:

Step 1: Choose 8bit color image, if the image have some meaning, in other word contain numbers of colors, because the selection of pixels depend on the location of bits 8,7,6,5,4,3,2,1 and the numbers of levels in the tree as 8,7,6,5,4,3,2,1,0.

Step 2: build the tree that contains the following record

```
PixelRec = Record {Col: Integer; Row: Integer}
Rec = Record {
            NodeNum: Integer;
            PixelNum: Pixelrec;
            BinData: integer;
            PixelColor: Byte;
           }
```

The NodeNum, PixelNum, BinData, PixelColor represent number of node, location of pixel in image and selected bit as zero or one respectively.

Step 3: Search into all pixels image to find the suitable pixel. In first level of tree the searching depend on the eighth bit in the pixel. Through searching, the first pixel have 0 should be choosing then must be added to left node of seed node, which has ”node number 2”, then break the loop and begin from first pixel in image to choose the first pixel have 1 then add it to right node of seed node, which has “node number 3”. In this step level number is 0 and all level is 8 then 8-0 = 8 so the condition depends on bit number 8 as 0 or 1 as shown in Fig. 2.

Searching process in the second level of the tree depends on the seventh bit in the pixel. Through searching, first pixel have 0 should be choosing then must be added to left node of node number 2 which has “node number 4”, then break the loop and begin from first pixel in image to choose the first pixel have 1 and add it to right node number 2 which has“ node number 5 ”. In this step level number is 1 and all level is 8 then 8-1 = 7 so the condition depend on bit number 7 as 0 or 1 as in Fig. 3.

And so on to another level {2…8}, but there exist another condition, the pixel which selected and inserted into the tree must be unique, did not choose it in another time:

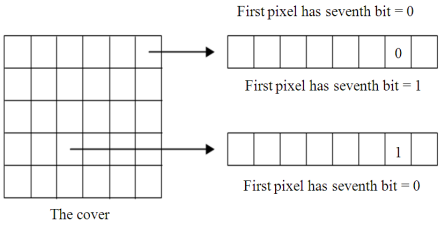

Fig. 3: Search to build second level in the tree

Step 4: Is enter the characters of secret message then convert it to binary and compare it as each character "contain 8 bit" with 8 bits in the branch then if the result true the secret key is number of pixel in the leaf of this branch, else move to another branch and so on. All of above steps is the embedding data and build the tree.

Step 5: Is Extracting the secret message from the image by enter the secret key which go direct to node has the same pixel number. Divided the node number on 2 to back to parent node and so on until node number = 1 then take each binary from each node then convert it to character.

RESULTS AND DISCUSSION

There are a number of important characteristics that a watermark can exhibit. Where the watermark should not be noticeable to the viewer nor should the watermark degrade the quality of the content, so the importance properties to keeping hidden information "secret message" (Similarity, Entropy, Robustness).

Similarity: The similarity is an important property of hiding information which the stego-cover and the original cover should not be distinguishable by the human or by the computer. The perfect methods are pure hiding information (Katzenbeisser and Petitcolas, 2002), where T(s) become equal one.

Hence embed process making selection bits from the image and did not make any change in the pixels so S(c/c): = 1, all pixels [I, J] of cover = pixels [I, J] stego-cover. In this study Distribution Key in Eight Bits Color Image Algorithm, is one of pure hiding information. Where the tree build depend on selection bits which did not changed as in Fig. 4.

Entropy: Entropy is a function to analyses the distribution of colors in the cover image and the stego-object, then compare between it. The Entropy function used by different type of attacker to discover if the cover contain hidden information or not (Katzenbeisser and Petitcolas, 2002), which E become equal the number of changed pixels divided on the summation of all pixels in the Stego-cover. In this study Distribution Key in 8bit Color Image Algorithm, Entropy becomes equal zero where no changed pixels exist as in Fig. 5.

Fig. 4: Similarity between original cover and stego-object

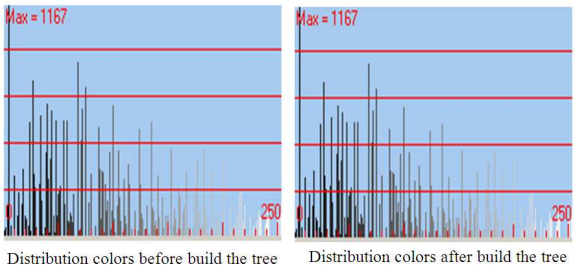

Fig. 5: Distribution colors where entropy = zero

Robustness: The selected keys chosen from pixels which distributed in image, where does not exist any changed on cover image so any updating on image doesn't mean anything, the key of owner it cannot known. There are several types of watermarking. Depending on the application, some basic types of attack are:

Robustness Attacker: which the aim to remove the presence of text watermarking (Cox *et al*., 2000), but in this algorithm the similarity = 1, so any changed such as compression, rotate and filtering and so on may be damaged the image but the attacker in any way cannot known the watermarking text.

Presentation Attacker: which modify the contents such that the detector to find the location of secret message (Miller *et al*., 1999). But also it cannot, to the same reason.

Interpretation Attacker: where an attacker can devise a situation which prevents assertion of ownership (Miller *et al*., 1999). Also this type of attacker cannot devise any situation because doesn't exist any relationship between the selected pixels and addition to this pixels it's distributed in different location in cover image.

CONCLUSION

Distribution key in eight bits color image algorithm one technique of pure hiding watermarking "Text in Image "by selecting pixels under some

condition. which the private key is “number pixel in the leaf node “ and the public key is “ tree which stored all selected pixels”, which can be give large numbers of secret key to different owners to the same image. Our future study is to develop the algorithm using 24, 32bit color images which the tree become have 24,32 level and each branch represent 3,4 characters respectively to obtain smallest private key and give the user more controlling on image type.

REFERENCES

Alshamasin, M., R. Al-kasasbeh, A. Khraiwish, Y. Al-shiboul and D.E. Skopin, 2009. Acceleration of image processing using new color model. Am. J. Applied Sci., 6: 1015-1020. DOI: 10.3844/ajassp.2009.1015.1020

Aliwa, M.B., T.E. El-Tobely, M.M. Fahmy, M.E.S. Nasr and M.H.A. El-Aziz, 2010. A new novel fidelity digital watermarking based on adaptively pixel-most-significant-bit-6 in spatial domain gray scale images and robust. Am. J. Applied Sci., 7: 987-1022. DOI: 10.3844/ajassp.2010.987.1022

Ramirez, C.B., M.N. Miyatake and H.P. Meana, 2004. Adaptive watermarking algorithm for binary image watermarks. Lec. Notes Comput. Sci., 3034: 207-216, DOI: 10.1007/978-3-540-24681-7_23

Miller, M.L., I.J. Cox, J.P.M.G. Linnartz and T. Kalker, 1999. A Review of Watermarking Principles and Practices. Digital Signal Processing for Multimedia Systems, Parhi, K.K. and T. Nishitani (Eds.), Marcel Dekker, Inc., New York, pp: 461-486, ISBN: 0824719247

Cox, I.J., M.L. Miller and J.A. Bloom, 2000. Watermarking applications and properties. proceeding of the International Conference on Information Technology: Coding and Computing, 27-29 Mar, IEEE Xploor, Las Vegas, pp: 6-10, DOI: 10.1109/ITCC.2000.844175

Delaigle, J.F., C. De Vleeschouwer and B. Macq, 2002. A psychovisual approach for digital picture watermarking. J. Electr. Imaging, pp: 1-29.

Findik, O., I. Babaoğlu and E. Ülker, 2010. A digital robust image watermarking against desynchronization attacks. Sci. Res. Essays, 5: 2289-2294.

Holtz, K.E., E.S. Holtz and D. Holtz, 1996. Autosophy information theory provides lossless data and video compression based on the data content. Proc. SPIE 2952: 518, DOI:10.1117/12.251313

Ismail, A., M.A. Shourman, K. M. Hosney and H.M. Abed Salam, 2010. Invariant image water marking using accurate zernike moments. J. Comput. Sci., 52-59. ISSN: 1549-3636

Katzenbeisser, S. and F.A.P. Petitcolas, 2002. Defining Security in Steganography Systems. pp: 1-7.

Liu, C.J., C. Hsing Lin and L.C. Kuo, 2006. A robust full-band image watermarking scheme. Proceeding of the International Conference on Communication systems, ICCS, 10th IEEE Singapore, Oct, IEEE Xploor, Singapore, pp: 1-5, DOI: 10.1109/ICCS.2006.301413

Ramesh, S.M. and A. Shanmugam, 2011. Comparison and analysis of discrete cosine transform based joint photographic experts group image compression using robust watermarking algorithm. Am. J. Applied Sci., 8: 63-70. DOI: 10.3844/ajassp.2011.63.70.

Al-Hunaity, M.F., S.A. Najim and I.M. El-Emary, 2007. Colored digital image watermarking using the wavelet technique. Am. J. Applied Sci., 4: 658-662. DOI: 10.3844/ajassp.2007.658.662.

Trappe, W., J. Song, R. Poovendran and K.J.R. Liu, 2001. Key distribution for secure multimedia multicasts via data embedding. IEEE ICASSP, pp: 1449-1452.

Van Schyndel, R.G., A.Z. Tirkel and C.F. Osborne, 1994. A digital watermark. Int. Conf. Imag. Proc.. 2: 86-89. DOI: 10.1109/ICIP.1994.413536

Wolfgang, R.B. and E.J. Delp, 1996. A watermarking for digital images. Int. Imag. Proc. , 3: 219-222, DOI: 10.1109/ICIP.1996.560423

Yang, Y. and X. Sun, H. Yang, C.T. Li, R. Xiao, 2009. A contrast-sensitive reversible visible image watermarking technique. IEEE Trans. Syst. Video Technol., 19: 656-667, DOI: 10.1109/TCSVT.2009.2017401