A Simple Approach on Image Authentication Watermarking

Dharamvir
Asst. Professor, Dept. of MCA
The Oxford College of Engineering
Bommanhalli , Hosur Road , Bangalore-68

ABSTRACT

An ideal watermarking scheme is a technique of embedding secret information into the image in order toauthenticate the image. This helps in detecting The integrity of the image. Here a block based Watermarking technique has been sed. A Fuzzy C means based algorithm is used here to Watermark and authenticate the image Experimental result here show that it can detect maximum modification and it can remove such changes done to the image.

Keywords*:* Image authentication, detection watermarking**.**

1 INTRODUCTION

An Ideal watermarking system is used to embed an amount of information that could not be removed or altered without making the cover object entirely unusable. A digital watermarking is a piece of information which is embedded in the digital media and hidden in the digital content in such a way that it is inseparable from the data. These water marks may be visible or invisible. But when we water mark the object it should not deteriorate the overall quality of the object. Invisible watermarks are inserted into documents to trace a possible illegal use.

The working principle of the watermarking technique is similar to the stegonography method. The figure shows the watermark embedding system.

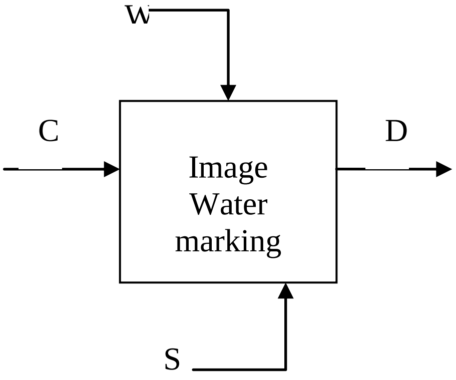
Where

C - Input Image

D – Watermarked Image

W – Watermark

S- Secret key



Watermark embedding System

The secret key here is used to enforce security to the image , which prevents the unauthorized parties from manipulating the Image or recovering the watermark .

1.1 Properties of watermarking:

There are number of important properties that watermark exhibit. Some of the important ones are given below:

*** Robustness:**

Robustness describes how well watermarks survive common signal processing operation. The Image may have to undergo variety of distortion.

*** Fragility:**

In some cases we may have to allow the user to copy or use the data may be image or the text or others, without any alteration to them. But any small alteration could destroy the watermark inserted into it. Thus if not detected, it can be ascertained that the object has been altered and necessary steps can be taken to regain the original modification by removing those changes to the object.

*** Fidelity:**

The fidelity of a watermarking system refers to the perceptual similarity between the original and watermarked versions of the input object.

*** Tamper resistance:**

A successful attack on the watermark system can damage or completely remove a watermark. Anticipation of such attacks and resistance against them comes in the tamper detection and tamper removal category.

2 Fuzzy C-Means Clustering (FCM) [2]:

A fuzzy C means is one of the unsupervised grouping technique. Here each point has a degree of belonging to clusters, as in fuzzy logic, rather than belonging completely to just one cluster. Thus, points on the edge of a cluster may be *in the cluster* to a lesser degree than points in the center of cluster. For each point x we have a coefficient giving the degree of being in the kth cluster $u_k(x)$. Usually, the sum of those coefficients for any given x is defined to be 1:

$$\forall x \left(\sum_{k=1}^{\text{num. clusters}} u_k(x) \ = 1 \right). \qquad \ldots.1$$

With fuzzy *c*-means, the centroid of a cluster is the mean of all points, weighted by their degree of belonging to the cluster:

$$\mathrm{center}_k = \frac{\sum_x u_k(x)^m x}{\sum_x u_k(x)^m}. \quad \text{….2}$$

The degree of belonging is related to the inverse of the distance to the cluster center:

$$u_k(x) = \frac{1}{d(\mathrm{center}_k, x)}, \quad \text{….3}$$

then the coefficients are normalized and fuzzyfied with a real parameter *m* > 1 so that their sum is 1. So

$$u_k(x) = \frac{1}{\sum_j \left(\frac{d(\mathrm{center}_k, x)}{d(\mathrm{center}_j, x)}\right)^{2/(m-1)}}. \quad \text{….4}$$

For *m* equal to 2, this is equivalent to normalizing the coefficient linearly to make their sum 1. When *m* is close to 1, then cluster center closest to the point is given much more weight than the others, This algorithm is similar to *k*-means.

The fuzzy *c*-means algorithm :

- Choose a number of clusters.
- Assign randomly to each point coefficients for being in the clusters.
- Repeat until the algorithm has converged (that is, the coefficients' change between two iterations is no more than ε, the given sensitivity threshold) :
- Compute the centroid for each cluster, using the formula above.
- For each point, compute its coefficients of being in the clusters, using the formula above.

The algorithm minimizes intra-cluster variance as well, but has the same problems as *k*-means; the minimum is a local minimum, and the results depend on the initial choice of weights. This FCM can also be considered as expectation-maximization algorithm. It is a more statistically formalized method which includes the idea of partial membership in classes. It has better convergence properties than other clustering algorithms.

3 Proposed scheme [1]:

3.1 Authentication Data Embedding :

Without loss of generality here we are adding the secret information into the image. For this reason, assume that the original host image H is a 8-bit grayscale image of size M × M pixels, where M is assumed to be an even number. The original image is divided into non-overlapping 2 × 2 blocks B_j (1 ≤ j ≤ M /2 × M/ 2) which are arranged by the order from left to right and then top to bottom.

To generate and embed the authentication data, the two LSBs of all the pixels within each block are first set to zero. Each block B_j can be regarded as a 4-dimensional vector, Bj=(B_{j1}, B_{j2}, B_{j3}, B_{j4}), where B_{jk}(1 ≤ k ≤ 4) represents a pixel color within block B_j. The FCM clustering is then applied to classify all the blocks into C clusters. After performing the FCM clustering, a membership matrix U of size C × (M/ 2 × M/ 2) is acquired, in which jth column indicates the membership degrees between block B_j and all the C clusters. For each column in U, the C membership degrees are rearranged in a descending order to obtain a new membership matrix ^U. A feature sequence F = {f_1, f_2, . . . , $f_{M/2\times M/2}$} can be generated from ^U by

$$f_j = \lfloor(\hat{u}_{1j} - \hat{u}_{Cj}) \times 255\rfloor, \quad 1 \leqslant j \leqslant \frac{M}{2} \times \frac{M}{2}, \quad \text{…. 5}$$

where ^u_{1j} and ^u_{Cj} represent the maximum and minimum values of jth column in ^U, respectively, and . denotes the floor operation. $\lfloor\ \rfloor$

Now we need to generate the random sequence of R={ r_1,r_2,… $r_{M/2\times M/2}$} using the pseudorandom number generator technique seeded with a secret key SK, where 0≤r_j ≤ 255. For each block B_j the corresponding authentication data a_j is constructed by the the following formula :

$$a_j = f_j \oplus r_j \quad \text{…. 6}$$

where the symbol $\oplus$ denotes the exclusive or operation. The resultant authentication data is now embedded into the 8 LSBs of the corresponding image block, and the watermarked image is obtained. Here the secret key SK and the cluster center information need to be kept secret by the owners for further tamper detection.

3.2 Tamper detection:

The possibly distorted image H", as in the authentication data embedding procedure, is first divided into non-overlapping 2 × 2 blocks B $_j$" (1 ≤ j ≤ M /2 × M 2). By verifying the authentication data embedded in each image block, we can determine whether a image block has been tampered with. To perform tamper detection, the embedded authentication data sequence, A = {a_1, a_2, . . . ; $a_{M2\times\_M2}$ }, is extracted from all the blocks of image H", and then the two LSBs of all the pixels within each block are set to zero. A membership matrix U" of size C × (M/ 2 × M/2) can be acquired by employing the following membership function, together with the weighting exponent m and the set of cluster centers V kept by the image owner, to all blocks

$$u''_{ij} = \frac{1}{\sum_{k=1}^{C}\left(\frac{\|B''_j - v_i\|}{\|B''_j - v_k\|}\right)^{\frac{2}{m-1}}}, \quad 1 \leqslant i \leqslant C, \quad 1 \leqslant j \leqslant \frac{M}{2} \times \frac{M}{2}, \quad \text{…. 7}$$

where C is the number of cluster centers contained in V. For each column in U", the C membership degrees are sorted in a descending order to obtain a new membership matrix ^U" . A feature sequence F" ={ f_1", f_2", . . . ; f"$_{M2\times\_M2}$ } can be derived from ^U" by utilizing Equation 5

Now we need to generate the random sequence of R={ $r_1,r_2,\ldots r_{M/2\times M/2}$} using the pseudorandom number generator technique seeded with a secret key SK that is secured by the owner, where $0\leq r_j \leq 255$. The authentication data sequence A”={$a”_1$, $a”_{2,}$ . . . , $a”_{M/2\times M2}$ } corresponds to image H” can be computed by applying F” and R to Equation 6

Finally, the legitimacy of each block $B”_j$ can be recognized by comparing $a”_j$ with a_j. If they are the same, $B”_j$ is a legitimate block; otherwise, it is regarded as a tampered block.

3.3 Tamper Removal :

The tamper detection algorithm here detects and highlights the area that has been tampered in the image. Now the OR operation can be applied between the two images i.e the original watermarked image and the tampered image, to remove the tampering from the image and regain the original image back for further processing.

4 Conclusions:

The proposed scheme authenticates the and thus helps in checking the integrity of the image. This system not only recognizes the integrity also recognizes and highlights the area where the image has been tampered. Based on this results one can decide the further steps. The same data can be used to authenticate the minimal watermarking detection for all the system needs. By using the cluster center we can change the application enhancement for improving the watermarking techniques. This proposed system also provides the opportunity for removing the changes done to the image and regaining the original one with no loss of information. The experimental result has yielded the satisfactory results. But the draw back of this proposed system is, it does not give 100 % accuracy, it can do only 99% tamper detection.

6 Experimental Result :

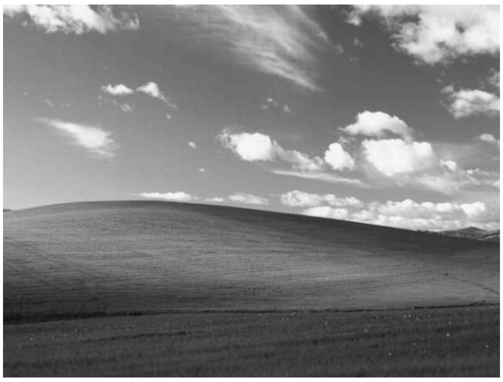


Fig 2: Original watermarked image

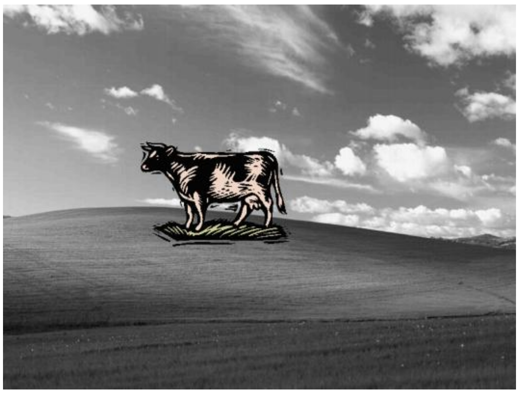


Fig.3 : Tampered Image

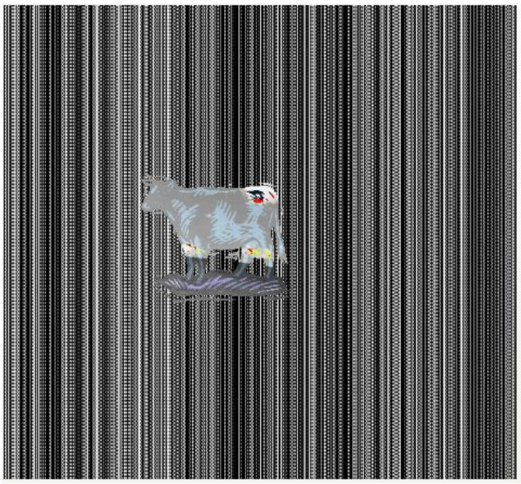


Fig. 4: Tamper detection result

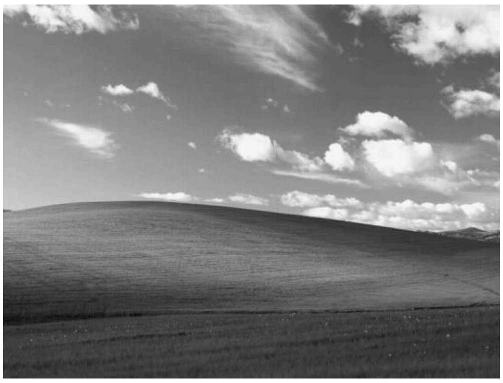


Fig 4: Regained image after removing the modifications.

5. REFERENCES

[1]. Wei-Che Chen, Ming-Shi Wang, "A fuzzy c-means clustering-based fragile watermarking scheme for image authentication", ScienceDirect, Experts System with Applications (2008) .

[2]. Liyan Zhang (2001), " Comparison of Fuzzy c-means Algorithm and New Fuzzy Clustering and Fuzzy Merging Algorithm ".

[3]. Bhattacharjee, S., & Kutter, M. (1998). "Compression tolerant image authentication". In Proceedings of IEEE international conference on image processing (pp. 435–439).

[4]. Celik, M. U., Sharma, G., Saber, E., & Tekalp, A. M. (2000). "Hierarchical watermarking for secure image authentication with localization". IEEE Transactions on Image Processing, 11(6), 585–595.

[5]. Chang, C. C., Hu, Y. S., & Lu, T. C. (2006). "A watermarking-based image ownership and tampering authentication scheme". Pattern Recognition Letters, 27(5), 439–446.

[6]. Eggers, J. J., & Girod, B. (2001). "Blind watermarking applied to image authentication". In Proceedings of IEEE international conference on acoustics, speech and signal processing (pp. 1977–1980).

[7]. Fridrich, J., Goljan, M., & Baldoza, A. C. (2000). "New fragile authentication watermark for images". In Proceedings of IEEE international conference on image processing (pp. 446–449).

[8]. Holliman, M., & Memon, N. (2000). "Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes". IEEE Transactions on Image Processing, 9(3), 432–441.

[9]. Kundur, D., & Hatzinakos, D. (1999), "Digital watermarking for telltale tamper proofing and authentication". In Proceedings of the IEEE special issue on identification and protection of multimedia information (pp. 1167–1180).

[10]. Li, C.-T., & Yuan, Y. (2006). "Digital watermarking scheme exploiting nondeterministic dependence for image authentication". Optical Engineering, 45(12), 127001.

[11]. Lin, C. Y., & Chang, S. F. (2000). "Semi-fragile watermarking for authenticating JPEG visual content". In Proceedings of SPIE conference on security and watermarking of multimedia contents II (pp. 140–151).

[12].Lin, E. T., Podilchuk, C. I., & Delp, E. J. (2000). "Detection of image alterations using semi-fragile watermarks". In Proceedings of SPIE conference on security and watermarking of multimedia contents II (pp. 152–163).

[13].Lin, P.-L., Hsieh, C.-K., & Huang, P.-W. (2005). "A hierarchical digital watermarking method for image tamper detection and recovery". Pattern Recognition, 38(12), 2519–2529.

[14].Lu, C.-S., & Liao, H.-Y. (2001). "Multipurpose watermarking for image authentication and protection". IEEE Transactions on Image Processing, 10(10), 1579–1592.

[15] Sachin Goyal, Roopam Gupta, Ashish Bansal, (2010) "A survey of digital watermarking with Genetic Algorithms". CSI Communications Journal, Volume No. 33.