Send Orders for Reprints to reprints@benthamscience.ae

456 *The Open Cybernetics & Systemics Journal*, 2015, *9*, 456-463

Open Access

Research on an Improved Algorithm for Image Authentication Signature AMAC

Yang Xinfeng[1,*] and Wei Ke[2]

[1]*School of Computer & Information Engineering, Nanyang Institute of Technology, Henan, Nanyang, 473000, P.R. China;* [2]*Zhongzhou University, Henan, Zhengzhou, 450044, P.R. China*

Abstract: The IAS based on the robust signature is studied and an improved AMAC (approximate message authentication code) is proposed. In this method, all the invariable bits of the image block referring to the threshold strength of incidental manipulation are used to construct AMAC. To locate malicious manipulation, a hierarchical AMAC is constructed. The robustness under JPEG compression and AWGN is investigated and its effectiveness is demonstrated.

Keywords: AMAC signature, image authentication, image edge, incidental manipulation, robust signature.

1. INTRODUCTION

The current robust image authentication technique can be divided into two categories: signature-based image authentication technique [1-6] and that based on watermarking image authentication [7-9]. In the case of watermark image based authentication technology, the image content may be relevant or irrelevant due to blind information hiding algorithm in the image and the image content authentication is equivalent to determine the image's hidden watermark information if changed [10-12]. In the signature-based authentication technology, some of the important images have a robust feature as the signature image and the image content authentication is equivalent to determine whether there have been changes in these important features. The former has the advantage that the user can be extracted directly from the image watermark authentication, having no additional bandwidth; the drawback is that during watermark induction, some distortion may occur. The advantage of the latter is that the images do not even need a small change that can better protect the visual quality of the image; the disadvantage is that it requires additional bandwidth for the transmission of the signature authentication information.

Signature-based image authentication verification can be divided into feature-based and image-based factor expression signature bits certification [13]. Kutter [14] used the Mexican hat wavelet extraction image feature point position with the distance between the image and the original image authentication feature point position being a decision function. Dittmna [15] coded information as a signature to the edges of the image, characterized by a variable length. Lin [1, 2] proposed a relationship between the size of the DCT coefficients based on the two images of the same location signature authentication technology with different image sub-blocks; the advantage of this algorithm is a strong ability to resist JPEG compression, but tampering with positioning accuracy is poor. Xie [3-6] has proposed AMAC (Approximate Message Authentication Code) based image signature verification technology, in which all images sub-block refers to the highest bit binary representation (MSB) of the composition of the image feature matrix of bits and features extraction matrix AMAC bit code as an image signature. Although the algorithm can resist PJEG within a certain range compression, its security is poor, and is easy to forge, tampering with poor positioning accuracy. Based on the above analysis, this article gives an improved AMAC image authentication technology; this relatively primitive algorithm has strong robustness, high positioning accuracy, leakage alarm probability and low probability of false alarm; moreover, a clear distinction between accidental and malicious attacks effectively overcomes the shortcomings of the AMAC image authentication technology.

2. MAC-BASED AUTHENTICATION TECHNOLOGY INFORMATION

MAC (Message Authentication Code) is a commonly used method in which authentication information can be divided into: Hash-MAC, Cipher-MAc and Approximate-MAC. The first two incorporate hard certification; even if relatively subtle changes occur in the information, MAC major changes may occur, and the degree of change in the information bits of the MAC is not directly linked. The latter belongs to soft certification, also known as the robustness of a signature; special information occurs when small changes, *i.e.* MAC small changes have taken place; the greater the degree of change in the information bits, *i.e.* MAC, the greater the probability of change. Hard certification refers to bit certification, while soft certification means content authentication. Hard certification is suitable for certification as it is more sensitive to the changes in information, such as text messages and so on. Soft certification is more appropriate for multimedia message authentication. Digital image data has a large amount of redundancy, distortion is not sen-

*Address correspondence to this author at the School of Computer & Information Engineering, Nanyang Institute of Technology, Henan, 473004, P.R. China; Tel: 13803770071; E-mail: ywind2005@163.com

1874-110X/15

Fig. (1). A) The original image. **B**) The tampered image. **C**) The certification results of Xie method.

sitive to the confidentiality of the low, easy to edit and modify the format and low range, so more suitable for image authentication AMAC. Xie [3] provided the AMAC authentication techniques which include the following three steps:

1. Configuration of the information bit sequence characteristics: $M(i), i = 1,..., Len$, $Len \le L \times R \times S$ wherein, L is AMAC code length, R, S is a positive odd number.
2. Standardization and scrambling operations. If the length of M is $Len < L \times R \times S$, thereafter adding 0, the length equals to $L \times R \times S$, and converting it into line $R \times S$, L column matrix, denoted by *M*, first column based on a pseudo-random number generator *P* generates a permutation of $\{1, 2,..., R \times S\}$, with scrambling results denoted as M_2, and then based on a random number generator *P*, a binary random matrix *N* is generated, which is denoted by $M_3 = M_2 \oplus N$, where $\oplus$ is OR operation.
3. While constructing AMAC, firstly, in every *R*-line, the main bit code is generated for each column, denoted by M_4, and then main-bit code is generated for each column of M_4, denoted by $A(i), i = 1,..., L$. A message is recorded as AMAC B's.

Every change in the probability AMAC signature *P*, depending on the ratio of the total length of the information bits is changed and the length of the original information bits satisfies: the larger the ratio of d_m / Len, *P* is the product. Xie [7,3] introduced that AMAC algorithm for image authentication has some disadvantages:

1. Original information selection: the most significant bit of $b_{i,j}$ is the feature bit to construct AMAC code $b_{i,j}$ holding that as long as there are remaining seven bits of tampering as constant, AMAC generated code will be identical. This is sufficient to destroy image content tampering. Fig. (**1A**) shows the original image, Fig. (**1B**) shows the tampered image, Fig. (**1C**) presents method for Xie authentication result; the white area is suspected of being the tampered area. Fig. (**1B**) is relative to the original image and the tampered regions are: A (8: 22,105: 153), B (171: 188,29: 46), C (221: 238,75: 91). While there are obvious differences in A region of the two images, and because the MSB of the mean of each corresponding image block in the region is the same, so the two AMAC are also the same. The method cannot detect the cause of Xie areas A, belonging to the missed event;
2. AMAC code generation function: The main function of majority in AMAC bit extraction code. This means that an attacker can arbitrarily tamper with the contents of a row or a column, or even in the most significant bit positions in the ratio of 0 and 1. So as long as the majority of the bits are unchanged, AMAC is able to generate the same code. Compared with the first case, this attack has a greater range of options. In actual testing, this causes the tampering detection probability to be lower than actual tamper detection probability theory, thereby reducing the performance of AMAC codes, resulting in missed events.
3. Positioning accuracy. When there are multiple areas in the image change, Xie's method tends to consider a lot of false alarm regions, that is why Xie's method can only determine whether the contents of a row or a column change, but not specific to image sub-blocks. According to Xie, when the image i-th row and j-th column AMAC signature changes, considering i-th row of the image, the j-th column of the image sub-block is tampered with, but this is not the case. Fig. (**1B**) shows that with respect to the original image, although only three regions were tampered with, Xie's method was suspected to have been tampered with four areas, two of which belonging to the false alarm region misjudgment.

In AMAC signature on the basis of information from the original and signature bits generated constructor function, this paper has proposed an improved digital signature scheme, which effectively overcomes the shortcomings of AMAC codes.

3. IMPROVED AMAC SIGNATURE CONSTRUCTION ALGORITHM

3.1. Minimum Constant Bit Theorem

With respect to the classical digital signature technology, the most notable features of the robust digital signature technology are: it can effectively distinguish malicious interference and occasional interference and has a strong adaptability. Image interference encountered during transmission can be divided into two categories: malicious interference and occasional interference. The purpose is to forge a malicious interference content of the image; for instance the image deceived recipients. Its characteristics include relatively concentrated area of attack, and strength; the approach is to replace and delete objectives; occasional interference generally does not change the content of the image with the aim to reduce the amount of data or redundancy, which is characterized by a large area of influence; the strength is weak, such as lossy compression and linear filtering. From a statistical perspective, malicious interference and occasional interference can be approximated as Gaussian noise mean equal to 0; the variance of σ_m^2 occasional interference is far less than malicious interference variance σ_{ma}^2. However, in practical applications, in order to clearly distinguish between malicious and accidental interference, interference can often be distinguished from the intensity of the operation, such as giving a characteristic change illustrates the value of T_d, when the interference intensity $|T| > T_d$, considering that the interference is malicious tampering, otherwise it is accidental interference. T may be a change of course, the intensity of the airspace, and may be change in the intensity of the frequency domain, adaptive selection according to the specific application, such as when the principal face of accidental operation of the image is a JPEG compression, the threshold T_d is the maximum that can tolerate quantization step size as the half. In signature-based image authentication algorithm design, in order to distinguish malicious tampering and accidental interference in the selection of feature bits, often $|T| \le T_d$, the local features extracted bits remain unchanged when $|T| > T_d$, while bits of the extracted feature change greatly.

Assuming that the image of a characteristic coefficient $s \in \left[0, 2^L - 1\right]$, which is binary $S = s_L s_{L-1} ... s_1$. Wherein, s_L is called the most significant bit (MSB), s_1 is the least significant bit (LSB). Noisy feature information $S' = S + T$, where T is the interference, S' is referred to as the binary representation of $S' = s_L' s_{L-1}' ... s_1'$. In order to characterize the information S, $|T| \le T_d$ interference in, S' relative to S change every bit as well as the minimum invariant feature location information of its binary representation, same article gives the lowest bit theorem; the specific content and certification process is as follows:

Theorem 1 (lowest constant bit theorem)

When $s_{k+1} = 0$, starting from the low to the high $k+1$ bit search, the first time $s_l = 1$ position denoted l.

When $s_{k+1} = 1$, starting from the low to the high $k+1$ bit search, the first time $s_l = 0$ position denoted l.

If $l = L$, S there are no minimum invariant bits; if $l > L$, S of the minimum constant bit is: $l_v = k + 2$.

If $l < L$, then $l_v = l + 1$. Meet: If $|T| \le T_d$, for any $m \ge l_v, s_m = s_m'$.

Corollary 1: S non-existent constant bit interval: $S \in \left[2^{L-1} - 2^k, 2^{L-1} + 2^k - 1\right]$. The probability $l_v = k + l + 2$ is 2^{-l}, wherein $l > 0$, $l_v = k + 2$ is the probability 2^{k+1-L}; there is no probability that the same bit: 2^{k+1-L}.

Corollary 2: The probability of interference when $|T| \le T_d$, S in the T interference, l_v-bit and higher bits are not changed, and when $|T| > T_d$, $\left[(n-1)q, nq\right]$ bit of S bit binary representation and higher position will not change for $P_{miss} = \dfrac{2^{l_v} - 2^{k+1} - 1}{2^L} \ne 0$

Corollary 2 shows that: when the feature changes strength as $|T| \le T_d$, l_v higher bit position will not change, and when $|T| < T_d$, T, not all will cause l_v-bit or greater change, to make the P_{miss} small, and l_v should be made as small as possible.

As can be seen, with respect to higher-order bits S strong anti-interference ability of the lower bits, according to Xie, the MSB refers image block as its invariant feature bits, but under normal circumstances, MSB does not completely represent all of the information S, and this results in a larger space for forgery attacker. In order to extract more information as the feature bits, resistance to interference of certain intensity is shown, typically using quantitative techniques, and the binary representation of the quantized result is referred to as the feature bits. But if a larger strength against accidental attack is required, quantitative techniques should be employed which will result in a large distortion of the original image. An important factor in this article is about each image block interference $|T| < T_d$, which features all the same bits as bits, in order to reduce the probability of a successful attack, but there are also some disadvantages: S corresponding different l_v may be different, while in the

event of interference, l_v will also change after *S*, while as can be seen from corollary 1, when $S \in \left[2^{L-1}-2^k, 2^{L-1}+2^k-1\right]$, there are no change bits, and in order to unify the minimum constant S bits of all, this paper based on the lowest constant bit small quantization distortion technique, the purpose of which is that the quantized coefficients are the same.

3.2. Based on the Lowest Constant-Bit Quantization

The main purpose is classical quantization data compression, *i.e.*, data representing a minimum number of data as much as possible, and this article aimed to quantify $Q_{new}(s)$, so that all quantitative results on interference $|T| < T_d$ invariant bits equal to l_v, it being as small as possible, and so in this condition, a small distortion is possible. This requires all interference $|T| < T_d$, $Q_{new}(s)$ to be minimum constant bit $l_v = k+3$. For calculation purposes, prior to quantization *S*, first rounding is required. Supposing $q = 4 \times T_d = 2^{k+2}$, $\left[(n-1)q, nq\right]$ integer interval *S* requires, for example, in this paper quantifying the function defined as follows:

$$Q_{new}(\mathrm{S}) = \begin{cases} (n-1)q + q/4 & S \in \left[(n-1)q, (n-1)q + q/4\right] \\ S & S \in \left[(n-1)q + q/4, (n-1)q + 3q/4\right] \\ (n-1) + 3q/4 - 1 & S \in \left[(n-1)q + 3q/4, nq\right] \end{cases} \quad (1)$$

Error is an important indicator to measure the performance of the quantitative techniques. The following error quantization techniques are described herein and classical quantization technique is compared. For classical quantization techniques, such that when the interference intensity $|T| \le T_d = 2^k$, the extracted feature bits remain unchanged, the quantization step size m must meet: $m \ge 2 \times T_d$, considering the smallest $m = 2^{k+1}$, in the interval $\left[(n-1)q, nq\right]$, for example, if the note quantization error for $e = Q - Q(S)$, then a method of quantifying errors e_{new} in this paper and classical quantization error method e_{old} variance W and R are as follows:

$$E\left(e_{old}^2\right) = \left(\sum_{k=0}^{k=q-1} \left((n-1)q + k - Q_{old}\left((n-1)q + k\right)\right)^2 \right) \Big/ q = 2 * \left(\sum_{k=1}^{q/4} k^2 + \sum_{k=1}^{q/4-1} k^2 \right) \Big/ q \quad (2)$$

$$E\left(e_{new}^2\right) = \left(\sum_{k=0}^{k=q-1} \left((n-1)q + k - Q_{new}\left((n-1)q + k\right)\right)^2 \right) \Big/ q = 2 * \sum_{k=1}^{q/4} k^2 \Big/ q$$

It is assumed that S satisfies characteristics evenly distributed. Obviously, the variance of the quantization error of e_{new} small article. Mainly because each quantization interval for the classic quantitative techniques to quantify the results of only one value, the method of this paper is different, it can take more than one value, as long as you can meet the minimum bits $l_v = k+3$. Next $k=1, L=8$, 0 and 31 for example, to quantify the results shown in Fig. (**2**). "." Which point to the original point, "*" for the algorithm to quantify the results of this paper, "+" for the classical algorithm to quantify the results, quantitative methods in this article have the following characteristics:

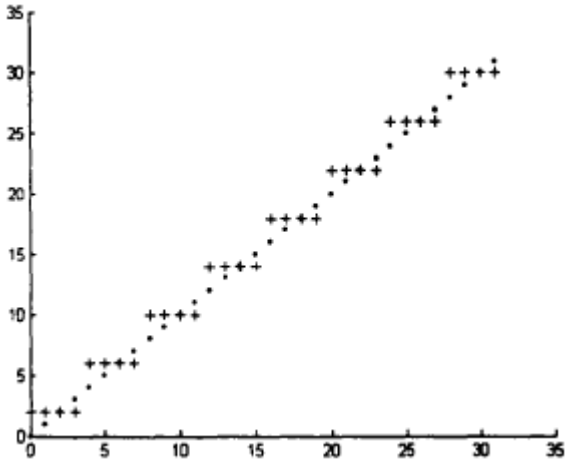

Fig. 2. (A) Classical quantitative method.

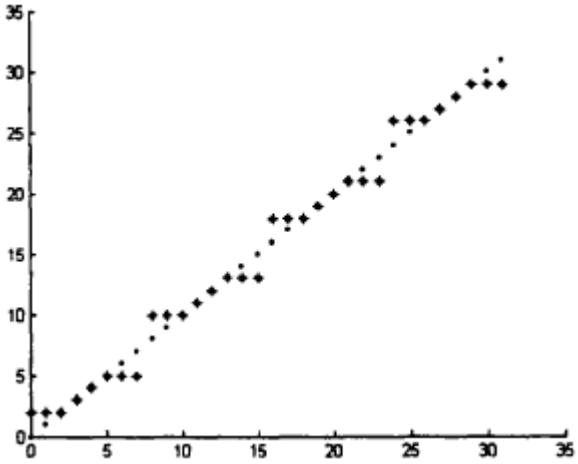

Fig. 2. (B) Quantitative method in this article.

1. The error variance is small. With respect to the size of the same T_d, $E(e_{new}^2) < E(e_{old}^2)$;
2. The value diversification. For the quantization step size *m*, $Q_m(S)$ is the number of possible values for $2^L/m$, and the algorithm has a certain stability, regardless of how much to take T_d, the number of possible values $Q(S)$ is 2^{L-1};

3. The ability to self-test error. $k+1$ bit on the binary representation of s_{k+1}, $k+2$ and s_{k+2} bits are satisfied: $s_{k+2}+s_{k+1}\equiv 1$.

3.3. Information Bits Feature Extraction and AMAC Signature Structure

Extract feature information for the performance of the algorithm plays a decisive role. The main image information epitome should meet the following requirements:

1. Sensitivity. Feature bits must not accept image processing operations with high sensitivity;
2. Robustness. Feature bits must have an acceptable robustness of image processing operations;
3. Locally. Feature bits must reflect the local features of an image;
4. Representative. When the feature bits change, the content of the image block considered is completely changed.

Image content changes inevitably lead to changes in the feature information; however feature information does not change the image content. Sensitivity and stability are a basic requirement of a robust image authentication, with the aim to distinguish between accidental operation and malicious attacks. System against malicious tampering positioning capability depends on the locality. Representation is the basis for image authentication. MSB bit features include robustness and better locality, but it is less sensitive and representative. MSB is only a part of the image content, and does not represent the main content of the image. Almost all of the tampering results in the DC coefficients and low frequency coefficients of the DCT transform of the image change, and try to avoid accidental interference modifying them. In this paper, the DC coefficient is used so as to extract the object, of course, for safety which may include low-frequency coefficients.

MAC is a digital signature, which originates from the feature information; feature information is compressed and its role is to detect whether the feature bits change and change of location positioning feature bits occurs as a valid signature; bits constructor should also meet the following three requirements:

1. Sensitivity: The characteristic signature of the bits must be changed as the information bits are more sensitive. Xie adopted majority (.) sensitivity is weak, and only when a large proportion of the signature features information changes, AMAC may change;

Locality: When the change in a signature bit occurs or a few bits of the signature change, it can be determined as which features of the image sub-blocks of bits are changed;

2. Security: Under the premise of no key, it is difficult to estimate the characteristic signature bits or bit by bit estimated signature feature bits.

As can be seen, the sensitivity of the signature bit basic requirement and local authentication system for tampering detection and localization capability are dependent on the signature bits of the locality, while for safety reasons, bit information and bit unidirectional characteristic must also be generated by the signature. Xie has constructed a one-way AMAC signature bit, but the locality and the sensitivity are poor, mainly because the signature is based on the feature bits' AMAC rows and columns, so when a change in AMAC occurs, only a line or a column feature bits change; the specific features which the row or column of the image block of bits is changed, there was no way to know at the same time the security of the algorithm is low, prone to counterfeiting, an attacker as long as the majority of bits unchanged, attack can be realized, mainly due to AMAC function to extract the main bit majority (.) basis, but this function is too simple, , there are some flaws in the security.

AMAC probabilistic algorithm has a drawback which is that only when the characteristic features of a small number of bits in the bit are changed, the corresponding change in AMAC signature is too small. In order to improve the security and sensitivity, this study used HASH (.) Function and the majority (.) Function together. It can be proven: as long as the original information sequence in which a bit change occurs, then extracted by HASH (.) signature sequence at least half bit changes, therefore, HASH (.) zoom function may function change, thereby improving sensitivity signature constructor, to ensure any row or column to make minor changes will be reflected images from abstract sequence, and the function is more complex, the attacker is difficult to predict the output from the input bit signature bit, high security.

In order to improve the tamper localization accuracy, usually signature bit is constructed for each image block. But this has some disadvantages: Whether extraction or authentication, each time must be hw times HASH(.) calculation; the calculation is too large and vulnerable to attack the vector [4]. In order to reduce the amount of calculation and improve the security, this paper has presented a similar structure mehmet [5] grade AMAC signature algorithm approach. First, the original image is divided into image matrix size of 8 × 8; secondly, construction algorithm based on feature information is given in this paper to extract invariant features bit matrix: F(i,j), structural characteristics of the bit matrix of each row and each column AMAC signature bit sequences are MAC'_{col} and MAC'_{row}:

$$\begin{aligned} MAC'_{col} &= Major\left(Truncate(Hash(F(l,1),...,F(l,h)),2N+1)\right) \\ MAC'_{row} &= Major\left(Truncate(Hash(F(1,l),...,F(\mathrm{w},l)),2N+1)\right) \end{aligned} \tag{3}$$

Wherein, *Truncate*(.) represents a length of a period of interception of 2N + 1 bits from the obtained signature bits; Then, the feature size of the bit array is divided into four sub-feature matrix $w/2\times h/2$, and then it is calculated for each row and each sub-feature matrix for each column of the AMAC signature, continuing until each feature segmentation matrix containing only the $w/2^M\times h/2^M$ picture sub-blocks feature bits, M may be adaptively selected, the higher the greater the accuracy of M: Finally, the resulting MAC'_{col} and MAC'_{row} connected together to form the image AMAC classification signature.

4. BASED ON THECLASSIFICATION OF MAGE AUTHENTICATION AND PERFORMANCE AMAC

4.1. AMAC Image Classification Algorithm Based Authentication

AMAC classification based image authentication can be divided into two steps: finding a suspicious image blocks and identifying suspicious image blocks. First, the received image is divided into sub-blocks of size image matrix $Sub^{'}(i,j)$ into 8 × 8, and the bits 7 to 11 of each sub-block and DCT transform DC coefficients of binary representation are extracted, denoted as: $F^{'}(i,j), i=1,...,w, j=1,...h$, and the characteristics of the current image as a matrix of bits extract this feature matrix's AMAC each row and each column of the signature $MAC_c^{'}$ and $MAC_r^{'}$, and the corresponding row and column of the original signature for comparison of AMAC; if the i-th row and j do not match, then the sub-image $Sub^{'}(i,j)$ suspects image block and the block sequence is referred to as suspect image: $Sub^{'}(i_l,j_l), l=1,...,N$, where N is the suspect image block total. Experimental results show that not every $Sub^{'}(i_l,j_l)$ has been tampered with, there are some false suspect image blocks, and to exclude these suspicious image blocks, the image is divided into sub-block matrix $Sub^{'}(i_l,j_l)$; the image sub-block $Sub^{'}(i_l,j_l)$ is divided into 4 sub-image block sizes of $w/2\times h/2$, denoted by $Sub_l^{'}(i,j), l=1,...,N$. $Sub_l^{'}(i,j)$ determines whether each image block is suspicious, and if there is no discrepancy, this $Sub_l^{'}(i,j)$ is credible, otherwise this sub-image block is calculated by AMAC matrix each row and each column and AMAC and primitive compared to if the same, then the image blocks suspicious of this sub-image block matrix contains not actually been tampered with; if not identical, this image sub-block matrix is divided, until the image sub-block matrix $w/2^M\times h/2^M$ contains only one image sub-block; if the block has not ruled out the suspicious image, then it can truly be considered a tampered image block.

4.2. Tamper Detection Probability

Tamper detection probability is defined as Re in the region l having feature bits when $F(i,j)$ changes; the probability of a single signature AMAC code changes occurring is represented by P_{AMAC}. For simplicity, assuming the region Re intentional alteration as size 8N × 8N square area results in alteration of the $N2$ feature bits l change. Tampering with the corresponding region of the digital signature bits each row and column of bits of the N adjacent.

Without loss of generality, assuming that a change of the feature bits l and $F(i,j)$ is a random evenly distributed change in the region Re, therefore, the probability of occurrence of each feature in the region Re $F(i,j)$ bit change is: $P_F=l/N^2$. The probability of changing a single row or a single column occurring, P_{cl} is:

$$P_{cl}=1-\left(1-P_F\right)^N \tag{4}$$

According to HASH (.) found, the characteristic function of the original information sequence is changed one bit by HASH (.) Function to get a summary of the sequence has at least half of the bits to be changed, therefore, adapts to the random 2N + 1 bits also at least (.) half of change, a change from the majority of the probability function to extract the signature of at least 1/2, combined with the above equation, , we can see the probability of a digital single row or column of bits changing a bit signature as:

$$P_{AMAC}=1/2P_{cl}=\left(1-\left(1-P_F\right)^N\right)/2 \tag{5}$$

Obviously, when P_{cl} is small, the original signature algorithm constructed AMAC occurrence probability variation is small, and the structure of the improved algorithm of AMAC signature bits changes to at least 0.5, clearly superior to the original algorithm.

Thus, tamper detection probability P_{AMAC} has image region size N and length l. The larger the $P_F=l/N^2$, the larger the P_{AMAC}. For general tampering features, it can be assumed that half the bit is changed, namely $l=N^2/2$. Therefore in the area of 8N × 8N region, the probability of the digital signature row (column) bits changed is:

$$P_{AMAC}=1/2F_{cl}=\left(1-2^{-N}\right)/2 \tag{6}$$

For general Re in the case of an unknown area, the size of the entire original image is often referred to as tampered area, and when the discovery of the image AMAC signature changes, in order to further pinpoint malicious tampering, the image needs to be divided into four, then each sub-image AMAC block signature needs to be calculated, since the area of the image block into the original is 1/4, so P_F becomes 4 times the original probability, so P_{cl} is increased, resulting in increased P_{AMAC}. So when a large image blocks AMAC signature changes, with further refinement, the probability of P_{AMAC} will increase and not decrease, due to which, it appears that in the larger area, tampering is not found, and tampering loss phenomenon occurs in the thinning process.

Fig. (3). (**A**) Quantized image (**B**) Tampered image (**C**) Detection and localization results.

Fig. (4). (**A**) Median filter image (**B**) AWAN noise image (**C**) Lossy JPEG image compression.

Fig. (5). (**A**) Filtering certification results (**B**) AWGN noise certification results (**C**) JPEG noise certification results.

5. THE EXPERIMENTAL RESULTS

In order to verify the effectiveness of the proposed algorithm, we tested two aspects, including malicious tampering detection and localization capabilities and the ability to resist occasional interference. Accidental interference includes: median filtering, AWNG and JPEG compression for paper size 256 × 256 grayscale image as a test object. Interference threshold $T_d = 16$, image psnr quantized = 47.266, if using classical quantitative techniques psnr = 46.5514. Wherein, Fig. (**3A**) is an image after quantization, Fig. (**3B**) is tampered image (tampered area comprising: A(8: 22,105: 153), B(171: 188,29: 46), C(221: 238,75: 91). Fig. (**4**) shows an authentication result; white area may be tampered area, with respect to the original image authentication AMAC, this algorithm does not involve missed and false detection. Fig. (**4A**) shows the window size as 3 × 3 median filtered image, Fig. (**4B**) is encountered with zero, $\sigma = 10$ means AWGN noise interference image, and Fig. (**4C**) presents the quality factor Q = 18% of JEPG compressing images. Figs. (**4** and **5**) respectively correspond to the authentication result. Experimental results show that: The compression algorithms AWGN and PJGE have strong resistance, but resistance to the median filter is weak. This is because the value of the filter is nonlinear filtering, partial destruction of the image is large, significant differences exist with respect to the original

image; it is considered to be illegal tampering, reasonable, and generally a low-pass filtering and high pass filtering; linear filtering returns for occasional interference, while the median filtering is classified as malicious interference.

CONCLUSION

This paper discussed the signature-based image authentication techniques. With respect to the image authentication based on digital watermarking technology, its advantage lies in the certification process for the need to protect the visual quality of the image from the destruction of small and signature less information, but there are also some disadvantages, such as the attacker can easily obtain the need to protect the image signature information and poor positioning capability. Based on the above considerations, we proposed an improved image classification AMAC authentication technology based on the lowest constant bit theorem; signature algorithm improved the DC coefficients and low frequency coefficients with respect to sub-block image disturbance. All the similar bits as image sub-block feature bits have threshold T, and thus construct an image with a signature hierarchy AMAC positioning when using stepwise refinement tamper localization algorithm. The improved algorithm avoids the security flaws of the original signature algorithm, reducing the probability of false alarm and missed alarm probability algorithm, and analyzes the improved algorithm for JPEG compression and AWGN noise resistance accidental operation. The simulation results show that the improved algorithm outperforms the original algorithm AMAC.

CONFLICT OF INTEREST

The authors confirm that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

This work was financially supported by the Henan Science and Technology Key Project (122102210563 and 132102210215).

REFERENCES

[1] C.- Y. Lin, "A robust image authentication method distinguishing JPEG compression From Malicious Manipulation," *IEEE Transactions on Circuits and System of Video Technology*, vol. 11, no. 2, pp. 153-168, 2001.

[2] L. Xie, "Approximate image message authentication codes," *IEEE Transactions on Multimedia*, vol. 3, no. 2, pp. 242-252, 2001.

[3] L. X. R. F. Gvaremna, and G. R. Arce, "Approximate message authentication codes," *IEEE Transactions on Image Processing*, vol. 20, pp. 52-63, 2000.

[4] L. Xie, and G. R. Arce, "A class of authentication digital watermarks for secure multimedia communication," *IEEE Transactions On Image Processing*, vol. 10, no. 11, pp. 1754-1764, 2001.

[5] P. W. Wong, "Secret and public key image watermarking scheme for image authentication and ownership verification," *IEEE Transactions on IP*, vol. 10, no. 10, pp. 1593-1601, 2002.

[6] M. Holliman, and N. Memon, "Counterfeiting attacks on oblivious block-wise independent invisible watermaking schemes," *IEEE Transactions on IP*, vol. 6, pp. 432-441, 2000.

[7] M. U. CeliK, "Hierarchical watermarking for secure imgae authentication with localization," *IEEE Transactions on IP*, vol. 11, no. 6 , pp. 585-595, 2002.

[8] J. Fridrich, M. Goljan, and R. Du, "Invertile authentication, Security and watermarking of Multimedia Contents," In: P.W. Wong and E.J.Del, Eds., *Proceeding of SPIE 4314*, vol. 15, pp. 197-208, 2001.

[9] W. Ding, W. Yan, and D. Qi, "Digital image transformation and information hiding technology," *Chinese Journal of Computers*, vol. 21, no. 9, pp. 38-843, 1998.

[10] J. Zhang, and C. Zhang, "Digital watermarking for image authentication," *China Journal of Image and Graphics*, vol. 8, pp. 367-373, 2003.

[11] S. Bhattacharjee, and M. Kutter, "Compression tolerant image authentication," *IEEE International Conference on Image Processing*, vol. 1, pp. 435-439, 1998.

[12] J. Dittman, A. Steinmetz, and R. Steinmetz, "Content-based signature for motion picture authentication and content-fragile watermarking," *IEEE ICMCS*'99, vol. 25, pp. 209-213, 1999.

[13] D. Kundur, and D. Hatzinkaos, "Digital watermarking for telltale tamper proofing and authentication," *Porceedings of IEEE*, vol. 87, no. 7, pp. 1167-1180, 1999.

[14] L. Xie, and G.R. Arce, "A class of authentication digital watermarks for secure multimedia communication," *IEEE Transactions on Image Processing*, vol. 11, no. 10, pp. 1754-1764, 2001.

[15] P. W. Wong, and N. Memon, "Secret and public key image watermarking schemes for imgae authentication and ownership verification," *IEEE Transactions on Imgae Processing*, vol. 10, no. 10, pp. 1593-1601, 2001.

Received: September 16, 2014 Revised: December 23, 2014 Accepted: December 31, 2014