A Hybrid Approach for Content Based Image Authentication

Jinse Shin and Christoph Ruland
Chair for Data Communications Systems, University of Siegen, Hoelderlinstr. 3, Siegen, Germany

Keywords: Content based Image Authentication, Perceptual Image Hashing, Tamper Detection.

Abstract: Perceptual image hashing has received an increased attention as one of the most important components for content based image authentication in recent years. Content based image authentication using perceptual image hashing is mainly classified into four different categories according to the feature extraction scheme. However, all the recently published literature that belongs to the individual category has its own strengths and weaknesses related to the feature extraction scheme. In this regard, this paper proposes a hybrid approach to improve the performance by combining two different categories: low-level image representation and coarse image representation. The proposed method employs a well-known local feature descriptor, the so-called Histogram of Oriented Gradients (HOG), as the feature extraction scheme in conjunction with Image Intensity Random Transformation (IIRT), Successive Mean Quantization Transform (SMQT), and bit-level permutation to construct a secure and robust hash value. To enhance the proposed method, a Key Derivation Function (KDF) and Error Correction Code (ECC) are applied to generate a stable subkey based on the coarse image representation. The derived subkey is utilized as a random seed in IIRT and HOG feature computation. Additionally, the experimental results are presented and compared with two existing algorithms in terms of robustness, discriminability, and security.

1 INTRODUCTION

The advances in electronic devices, wireless mobile communication, and multimedia technologies have accelerated the explosive growth of multimedia traffic, so that the needs of a secure multimedia communication over wireless channels have been raised. However, the emerging security demands are difficult to be met by the standardized cryptographic methods (ISO/IEC9797, 2011; NIST-FIPS, 2013) or soft authentication methods (Graveman and Fu, 1999; Boncelet, 2006; Ur-Rehman and Zivic, 2013) since the security requirements of multimedia communication are different in many ways from those of the traditional data communication (Shin and Ruland, 2013).

The main difference from the security perspective is the definition of data integrity. The general definition of data integrity is to assure the binary representation of data has not been corrupted or modified during a data communication procedure, whereas data integrity in multimedia communication requires ensuring the perceptual content has not been manipulated even though its binary representation is completely different. For this reason, content based multimedia authentication approach has been considered as an attractive solution.

In this regard, perceptual image hashing has received an increased attention to authenticate the image content on a semantic level. There have been proposed several image authentication schemes based on the perceptual image hashing in the literature (Han and Chu, 2010; Haouzia and Noumeir, 2008). According to the type of feature extraction scheme, content based image authentication is largely classified into four different categories: Image statistics, relation, coarse image representation, and low-level image representation based feature extraction (Monga and Evans, 2006).

Although all the recently published literature within those categories can achieve good performance with respect to robustness against content preserving modifications, they possess their own limitations related to the feature extraction scheme. Thus, this paper proposes to combine two different types of feature extraction scheme: low-level image representation and coarse image representation. As a low-level image representation based feature extraction scheme, HOG feature descriptor is employed with IIRT, SMQT, and bit-level permutation not only to capture the local characteristics of an image but also

Shin J. and Ruland C..
A Hybrid Approach for Content Based Image Authentication.
DOI: 10.5220/0005059003710378
In *Proceedings of the 11th International Conference on Security and Cryptography* (SECRYPT-2014), pages 371-378
ISBN: 978-989-758-045-1

to construct a secure and robust hash. Likewise, a coarse image representation computed by the use of Discrete Cosine Transform (DCT) jointly with Singular Value Decomposition (SVD) is utilized to produce a subkey in conjunction with KDF and ECC. The derived subkey can be used as a random seed of the pseudorandom number generator used for IIRT and HOG feature computation to enhance the discriminability and security of the proposed method.

The rest of this paper is organized as follows. Section 2 briefly introduces some of the representative algorithms within each category and explains their security related issues. Section 3 presents the proposed method for content based image authentication using a hybrid approach, followed by experimental results with a discussion in section 4. Finally, the last section concludes the paper with a brief summary.

2 PRIOR WORKS

The basic idea behind content based image authentication approach is that it can be aware of the image content by constructing an image hash value from the invariant image features, and then generate a Message Authentication Code (MAC) or digital signature from it. Consequently, the feature extraction scheme affects the performance in terms of robustness and discriminability since the extracted features play a main role to distinguish between the malicious manipulations and acceptable content preserving modifications. Some representative algorithms of each category are reviewed in this section.

The approach using the image statistics based feature extraction computes the statistics of an input image such as mean, variance, and higher moments of intensity values as an invariant feature. (Venkatesan et al., 2000) proposed to utilize the statistics of Discrete Wavelet Transform (DWT) coefficients calculated from the randomly partitioned rectangles of each sub-band in wavelet decomposition of an image. Another scheme is approximate Image Message Authentication Code (IMAC) proposed by (Xie et al., 2001), which applies a cryptographic primitive Approximate Message Authentication Code (AMAC) (Graveman and Fu, 1999) on the most significant bits of 8×8 block average with image histogram enhancement. Although those schemes demonstrate good robustness against several content preserving modifications, they possess the limitation that an image can be easily modified without altering its image statistics.

The relation based approach exploits the invariant relationship between a pair of transform coefficients. As a representative scheme of this category, (Lin and Chang, 2001) proposed a robust image authentication method using the relationship between DCT coefficients at the same position in separate blocks of an image. Since this invariant property is derived from the fact that all DCT coefficients at the same position in DCT blocks are divided by the same quantization table during JPEG lossy compression process, it can achieve excellent robustness against JPEG compression. However, most of the AC coefficients in DCT block where the image has a smooth texture may become zero after JPEG lossy compression, so that the extracted features cannot be reliable for image authentication any more.

The approach based on the coarse image representation utilizes the invariance in the transform domain, which may preserve the significant characteristics of the image. (Mihcak and Venkatesan, 2001) applied a simple iterative filtering operation on the binary map of the DWT approximation sub-band to obtain the geometrically strong components. (Kozat et al., 2004) proposed another interesting image hashing algorithm which applies SVD to pseudo-randomly chosen semi-global regions of an image, then selects the strongest singular vectors to extract robust features. Compared to the other categories, this approach obtains better robustness under acceptable modifications. However, such an excellent robustness may lead to a false positive authentication with a high probability. Moreover, the iteration of their algorithms to capture the significant characteristics of an image requires a high computational complexity.

The low-level image representation based approach uses low-level image features such as edges or feature points, which are widely used for object or scene recognition in image processing domain. (Queluz, 1998) proposed an image authentication scheme that relies on image edges obtained by Sobel or Canny edge detector, whereas (Monga and Evans, 2006) proposed to extract visually significant image feature points by using end-stopped wavelet based feature detection algorithm. The main problem of the low-level image representation is that edges or feature points can be easily distorted by the quantization errors and other compression artifacts even though they are good at capturing the local characteristics of an image. In particular, the algorithms using feature points may not be able to detect the malicious manipulations since they select and use only the limited number of feature points retaining the strongest coefficients to construct an image hash. Accordingly, it is highly possible to add or remove a set of feature points for malicious manipulations while maintaining the same strongest feature points of an image (Hsu et al., 2009).

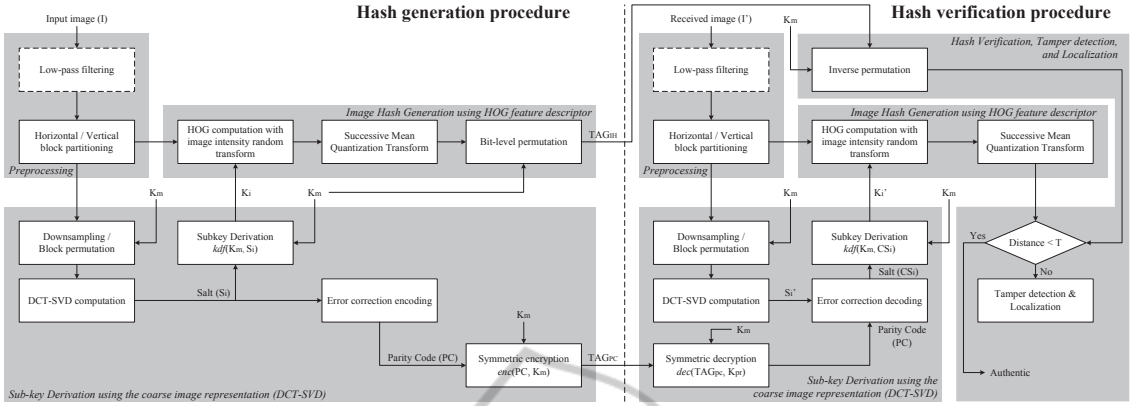


Figure 1: Block diagram of the proposed method.

3 PROPOSED METHOD

A hybrid method proposed in this paper is based on two main ideas: (a) HOG feature descriptor from a randomly transformed image by IIRT, (b) Subkey derivation from the coarse image representation in conjunction with ECC. Fig. 1 illustrates a block diagram of the proposed method, and the following subsections introduce each step of the hash generation and verification procedure.

3.1 Hash Generation Procedure

3.1.1 Preprocessing

A low-pass filtering can be optionally applied on an image to reduce the noise as a preprocessing operation. After that, the smoothed image is horizontally and vertically partitioned into a total of $(r+c)$ non-overlapped blocks, H_i $(1 \leq i \leq r)$ and V_j $(1 \leq j \leq c)$ with the size of $M' \times N$ and $M \times N'$ respectively, where $M' = \frac{M}{r}$ and $N' = \frac{N}{c}$ when the dimension of an input image is $M \times N$. Accordingly, all the blocks of an input image are represented by $\boldsymbol{I} = \{B_1, ..., B_{r+c}\} = \{H_1, ..., H_r, V_1, ..., V_c\}$.

3.1.2 Subkey Derivation

As a coarse image representation based feature extraction scheme, DCT-SVD hashing algorithm that demonstrates an excellent robustness is used with a slight modification (Kozat et al., 2004). The subkey derivation process using the modified DCT-SVD hashing scheme is described as follows.

(1) Perform downsampling on all the blocks B_i to halve the spatial dimension of an image. The dimension of downsampled B_i is $\frac{M'}{2} \times \frac{N}{2}$ and $\frac{M}{2} \times \frac{N'}{2}$ for the horizontal and vertical block respectively.

(2) Perform a sub-block permutation for each B_i after splitting the downsampled B_i into non-overlapped $p \times p$ sub-blocks. Let BP_i be the permuted block of the downsampled B_i.

(3) Compute 2D DCT for each block of $d \times d$ within BP_i, then take only the DC coefficient from them. DC_i for each BP_i is constructed by concatenating all the DC coefficients of all $d \times d$ DCT blocks within BP_i, and represented as $DC_i = \{DC_{i,1}, ..., DC_{i,j}\}$. $DC_{i,j}$ denotes the DC coefficient of j-th DCT block within BP_i, where $1 \leq j \leq \frac{M' \times N}{(2d)^2}$ for the horizontal block and $1 \leq j \leq \frac{M \times N'}{(2d)^2}$ for the vertical block.

(4) Apply SVD on DC_i and take the strongest singular vectors. The final coarse image representation S_i from each B_i is constructed by converting the vectors into the integer between 0 and $2^q - 1$, where q is the number of quantization bits.

(5) Given the final coarse image representation S_i acts as a non-secret parameter called 'salt' in KDF for B_i. Hence, a subkey K_i for each B_i is derived by $K_i = kdf(K_m, S_i)$, where $kdf(\cdot,\cdot)$ is a key derivation function with a master secret key K_m and salt S_i. Note that the proposed method does not depend on any specific type of KDF algorithms so that any standardized KDF can be adopted in the proposed method (NIST-SP, 2009; Krawczyk and Eronen, 2010).

(6) For the purpose of increasing robustness, convert S_i into a Gray code and encode each vector element within S_i using ECC to obtain the parity code bits PC_i. Note that the proposed method applies the Hamming code (n,k) that can correct single-bit errors, where n and k represent the length of output encoded message and original message respectively.

(7) Concatenate all the parity code bits of every S_i to construct $\boldsymbol{PC} = \{PC_1, ..., PC_{r+c}\}$. The final tag information concerning the parity code bits can be obtained by $TAG_{PC} = enc(K_m, \boldsymbol{PC})$, where $enc(\cdot,\cdot)$ denotes a symmetric encryption function.

As long as the coarse image representation S_i extracted in step (4) can be invariant under a certain level of distortions, KDF can produce the same subkey for each B_i in step (5) since S_i is utilized as a salt value in KDF. In this context, the proposed method employs Gray code conversion and Hamming error correction code in step (6) to obtain the stable salt value by correcting single-bit errors. Due to the locality of the distortion introduced by malicious manipulations, it is expected that the hamming distance between the coarse image representations in the Gray code is larger than one when the image is tampered. In this manner, S_i computed from the tampered image cannot be corrected whereas the one from acceptable modifications can be corrected. Thus, the use of single error correcting codes is much preferable than burst error correcting codes in the proposed method.

3.1.3 Image Hash Generation

HOG feature descriptor may make a false authentication decision when it is used for content based image authentication, since the image gradients can be distorted by the quantization errors and other compression artifacts. To cope with this problem, a method to randomly transform the image intensity before HOG computation is proposed in this paper. The followings present how to generate a final hash value using HOG feature descriptor.

(1) Apply IIRT given by equation (1) on every B_i, resulting in the randomly transformed image BT_i.

$$BT_i(x,y) = B_i{}^{\gamma}(x,y) + rand_{x,y}(K_i, r_{max}) \quad (1)$$

$B_i(x,y)$ and $BT_i(x,y)$ respectively represent the pixel intensity at the coordinate (x,y) in each block of B_i and BT_i, where $1 \le x \le M'$, $1 \le y \le N$ for the horizontal block and $1 \le x \le M$, $1 \le y \le N'$ in the case of the vertical block. $rand_{x,y}(K_i, r_{max})$ denotes a pseudo random number generator with a derived subkey K_i as a random seed, which generates a random number less than r_{max} at the position (x,y) of each block. Additionally, γ is a configurable parameter for Gamma correction.

(2) Compute HOG feature descriptor with a small modification of the original HOG feature descriptor (Dalal and Triggs, 2005): Firstly, the gradient magnitudes and orientations are calculated from each BT_i, followed by concatenating the sum of the gradient magnitudes within each orientation bin of the histogram. To eliminate the possibility of maliciously manipulating the image without altering HOG feature descriptor, each block is randomly re-partitioned into several sub-blocks. Afterwards, those sub-blocks are utilized as well in order to compute HOG feature descriptor as given by equation (2).

$$F_i = \left\| T_i + \sum_{j=1}^{NB} U_{i,j} \right\|_2 \quad (2)$$

T_i denotes the unnormalized HOG feature from the entire i-th block of BT_i, whereas $U_{i,j}$ is from the j-th sub-block randomly selected within BT_i, where NB is the number of sub-blocks and $\|\cdot\|_2$ represents the L2-norm operator. Concatenating the normalized HOG feature F_i of every BT_i results in the final HOG feature descriptor represented by $\boldsymbol{F} = \{F_1, ..., F_{r+c}\}$.

(3) Quantize the final HOG feature descriptor into 2^l levels, where l is the number of bits for quantization). As for the quantization process, SMQT is employed since it can remove a small perturbation of data by performing an automatic structural breakdown of data and building a SMQT binary tree (Nilsson et al., 2005).

(4) Permute the quantized HOG feature descriptor at bit-level and perform the XOR operation with pseudorandom bits. Finally, it constructs a final image hash, TAG_{IH}.

The use of IIRT is introduced to minimize a certain level of gradient distortions caused by lossy compression and noise, so that it helps to obtain more robust HOG feature descriptor. The impact of IIRT on robustness is presented by experiments in section 4.1. Additionally, IIRT helps to increase the security property by producing a perceptually same image but having different random representations and image gradients. To obtain more secure hash, a bit-level permutation step is employed (Xie et al., 2001) since it can prevent an attacker from estimating the relationship between any bit of TAG_{IH} and a specific image block or orientation bin. As a result, it is impossible to estimate or manipulate HOG feature descriptor from TAG_{IH} without knowing the master secret key.

3.2 Hash Verification Procedure

3.2.1 Preprocessing

As shown in Fig. 1, the received image is preprocessed in the same way as image hash generation procedure described in section 3.1.1. Thus, all the blocks of the received image are similarly represented by $\boldsymbol{I'} = \{B'_1, ..., B'_{r+c}\} = \{H'_1, ..., H'_r, V'_1, ..., V'_c\}$.

3.2.2 Subkey Derivation

The most challenging task to derive a correct subkey at the receiver is to obtain the same salt value from the received image. Firstly, the coarse image representation S'_i is extracted from each B'_i according to the steps (1)–(4) in section 3.1.2. Since S'_i can be considered as a noisy version of S_i, all the single-bit errors on S'_i can be corrected by Hamming decoder with the parity code bits PC_i. PC_i can be retrieved by $\boldsymbol{PC} = dec(K_m, TAG_{pc})$, where $dec(\cdot,\cdot)$ denotes a symmetric decryption function. As given by $K'_i = kdf(K_m, CS_i)$, a subkey K'_i can be derived from CS_i which is the corrected version of S'_i.

3.2.3 Image Hash Generation

At the receiver, it is not necessary to perform a bit-level permutation since HOG feature descriptor of the original image can be recovered from the received TAG_{IH} by applying the inverse permutation. Thus, the steps (1)–(3) in section 3.1.3 are only performed.

3.2.4 Image Hash Verification, Tamper Detection and Localization

HOG feature descriptor of the original image is retrieved from the received TAG_{IH} through the inverse permutation. A distance between the retrieved HOG feature descriptor and the one computed in section 3.2.3 is compared with a threshold to verify the authenticity and integrity of the received image. If the distance is less than the threshold, the received image will be declared as authentic. Otherwise, it will be considered as non-authentic, thus a tamper detection and localization step will be processed.

To identify the tamper regions on the received image, a Sum of Absolute Differences (SAD) between two HOG feature descriptors is calculated for each B'_i. The absolute differences of each orientation bin within HOG feature descriptor of B'_i will be compared with a threshold, then accumulated if the difference is larger than the threshold. In this manner, any B'_i where has non-zero SAD value are indicated as a candidate being manipulated. Finally, the intersection of all candidate blocks will be considered as a tampered area. Fig. 2 shows a tampered image and the result of the tamper localization on a given image.

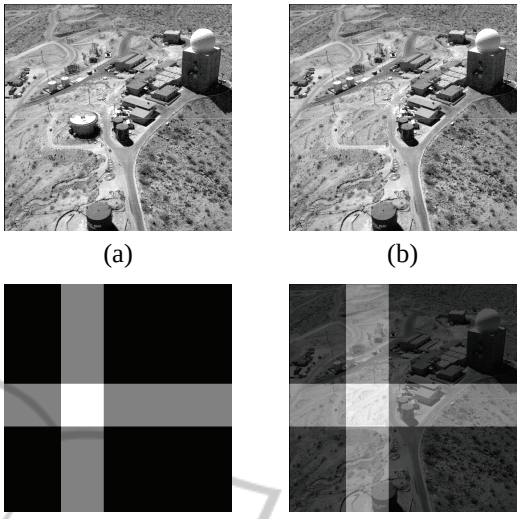


Figure 2: Example of tamper localization. (a) Original image. (b) Tampered image (Tampered region with a size of 80×80). (c) SAD map. (d) Tamper localized image.

4 EXPERIMENTAL RESULTS

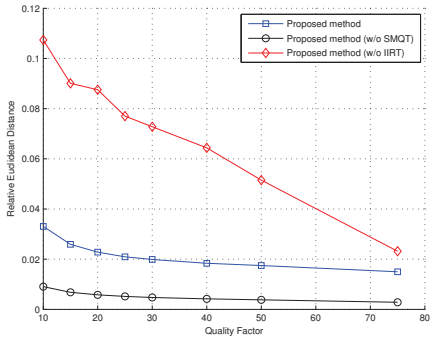
The proposed method is evaluated by experiments with respect to robustness, discriminability, and security. In experiments, 30 images (512×512 grayscale with 8-bit per pixel) from USC-SIPI database and their several modifications are used. As for the modifications, three types of allowable modifications – JPEG/JPEG2000 compression (QF between 10 to 75 and Compression ratio between 1:5 to 1:100 respectively) and Additive White Gaussian Noise (AWGN) over a Rayleigh-fading channel with Binary Phase Shift Keying modulation without using the channel coding (BER between 10^{-4} and 10^{-2}) – are applied. Besides, one image tampering operation that combines a part of another image with the original image dataset is adopted for content changing manipulation.

The algorithmic parameters of the proposed method are chosen as, $r = c = 16$ resulting in a total of 32 blocks (16 horizontal blocks of 32×512 and 16 vertical blocks of 512×32), $p = 8$, $d = 16$, $q = 8$, $n = 15$, and $k = 11$ for the subkey derivation process, $\gamma = 1.6$, $r_{max} = 640$, $NB = 64$, $l = 5$, and the number of orientation bins $= 9$ for the hash generation process.

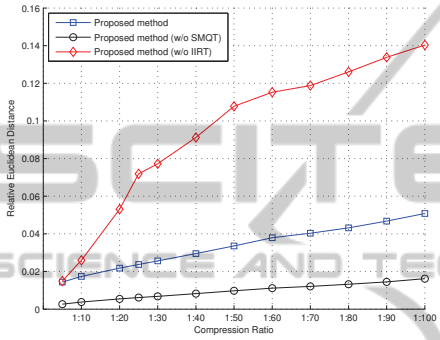
4.1 Robustness

Robustness is evaluated by measuring the relative Euclidean distance between HOG feature descriptors of the original and distorted images by acceptable modifications. Fig. 3 compares the results of the proposed method with others computed without applying IIRT or SMQT quantization to investigate the impact of IIRT and SMQT in the proposed method.

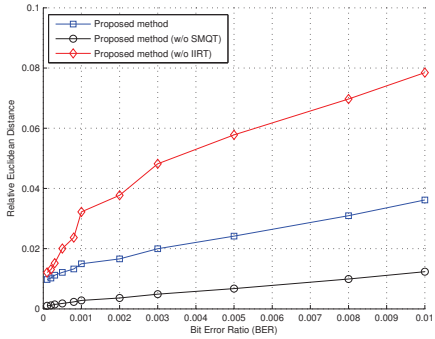
In the case of without applying IIRT, the distance increases significantly and reaches a peak of around 0.11, 0.14, and 0.08 respectively for image compres-



(a) JPEG compression.



(b) JPEG 2000 compression.



(c) AWGN.

Figure 3: Relative Euclidean Distance between HOG feature descriptors of the original and modified image for three approaches: Proposed method with IIRT (quantized by SMQT), Proposed method with IIRT (no quantization), and Proposed method without IIRT.

sions and AWGN as the compression and error ratio increase. However, applying IIRT before HOG computation improves the robustness by keeping the distance less than 0.02 through all the content preserving modifications when HOG feature descriptors are not quantized. It is also observed that the distance in the presence of SMQT quantization errors still remains relatively small – less than 0.04, 0.05, and 0.04 respectively – even though it slightly increases the overall distance.

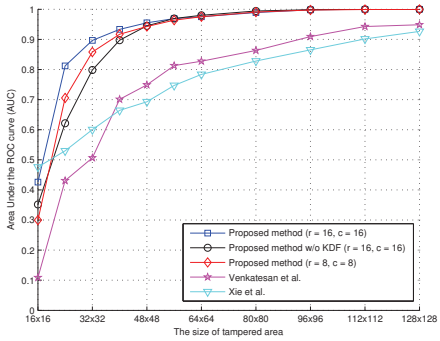


Figure 4: Discriminability comparison.

4.2 Discriminability

Discriminability is assessed by how well the proposed method can distinguish content changing manipulations from content preserving modifications. To do this, the distances between the original and manipulated images with various size of tampered region are compared with the results of content preserving modifications by applying Receiver Operating Characteristics (ROC) analysis. The experiments to investigate the influences of KDF and algorithmic parameters r and c are also conducted. More importantly, the performance of the proposed method is compared with two existing methods (Venkatesan et al., 2000; Xie et al., 2001) since both of them demonstrated a better discriminability than the other algorithms in (Shin and Ruland, 2013).

As presented in Fig. 4, the proposed method achieves excellent discriminability and even outperforms two existing methods. The influence of KDF is observed that applying KDF can improve discriminability especially when the size of tampered area is relatively small. For example, KDF increases the Area Under the ROC Curve (AUC) from 0.8 to 0.9 at the size of 32×32 and from 0.6 to 0.8 at the size of 24×24. As for the impact of the algorithmic parameters r and c which respectively represent the number of horizontally and vertically partitioned blocks, the results indicate that the larger r and c, the better performance can be achieved. However, there is a trade-off between the performance and the final hash length.

4.3 Security

To evaluate the security of the proposed method, this paper employs two desirable properties presented in (Coskun and Memon, 2006): (a) Confusion - The complexity of the relation between the key and the hash value, (b) Diffusion - The irrelevance between the perceptual information of the input and the hash

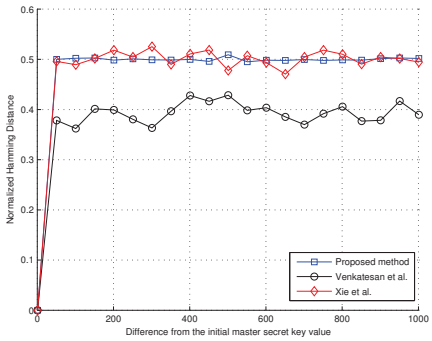


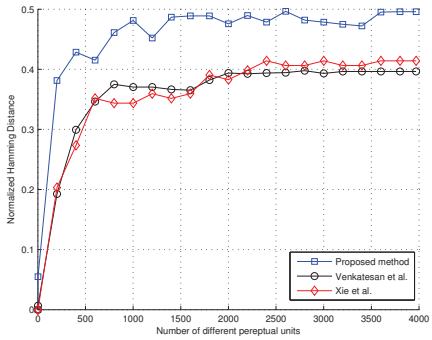
Figure 5: Normalized Hamming Distance of hash values under 1000 different master secret keys.

value. Thus, it is desirable that a small perceptual change on the image content or a single bit change of the secret key can cause a significant change on the output hash value. The experiments conducted in (Coskun and Memon, 2006) are reproduced.

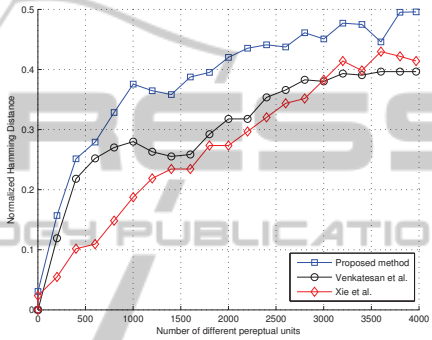
Concerning the experiments for the confusion capability, an initial master key is randomly selected and sequentially increased by one to generate 1000 different master keys. Afterwards, the final hash value calculated using the initial master key is compared with the ones obtained from other keys to verify the statistical irrelevance between them by measuring the normalized Hamming distance. Fig. 5 shows that the mean distance of all three methods stays around 0.50, 0.40, and 0.51 respectively, which indicates that they possess good confusion capability.

The diffusion capability is evaluated by measuring the normalized Hamming distance as the perceptual units of an image are gradually replaced with the corresponding units of another image in two different ways, either by random substitution or local substitution. The random substitution is to randomly select the perceptual units and replace them whereas the local substitution is to select a specific perceptual unit and grow the regions. Note that 16×16 blocks overlapped with ratio of $\frac{1}{2}$ in both horizontal and vertical direction is considered as the perceptual unit in the experiments.

As shown in Fig. 6, changing a single perceptual unit cannot result in a completely different hash value regardless of the substitution scheme due to the robustness property of the hash algorithm. In the case of the random substitution, however, the normalized Hamming distance of the proposed method significantly increases until reaching around 0.4 where 250 out of 3969 perceptual units are randomly substituted, and then slowly increases up to almost 0.5. On the other hand, the replacement of more than 1750 perceptual units is required for two existing methods in



(a) Random substitution.



(b) Local substitution.

Figure 6: Normalized Hamming Distance of hash values under two types of substitution.

order to reach the distance of 0.4. Compared to the random substitution, all three methods achieve much worse diffusion capability when applying the local substitution. Since most of the existing image hashing algorithms are designed to divide an image into several blocks and construct a hash value using robust features extracted from each block, it is obvious that the localized distortion produces a more similar hash value than the randomly distributed distortion. However, the experimental results show that the proposed method still outperforms the other methods.

5 CONCLUSIONS

In this paper, a hybrid approach combining HOG feature descriptor with the subkey derivation using the modified DCT-SVD hashing algorithm is proposed and evaluated in terms of robustness, discriminability, and security. HOG feature descriptor computed from the randomly transformed image by IIRT is used as the invariant features to achieve the robustness. On the other hand, the coarse image representation ob-

tained by the modified DCT-SVD hashing algorithm is considered as a salt value in KDF to derive a stable subkey in conjunction with ECC for each horizontal and vertical image block. The derived subkey is utilized as a random seed for each corresponding block during HOG feature computation. In such a way, the proposed method can improve the discriminability by producing a different subkey that will generate a totally different HOG feature descriptor for the manipulated block. Additionally, the security property of the proposed method mainly relies on the randomness introduced by IIRT, random re-partitioning, and bit-level permutation. The use of KDF also helps to provide better security by deriving a subkey from the image content and utilizing it as a secret key for each image instead of reusing the same master secret key for all the images. Thus, it can prevent an attacker from estimating the secret key based on the large number of image and corresponding hash value pairs.

Based on the experimental results, it is observed that the proposed method can successfully distinguish the malicious manipulations from the content preserving modifications while still having good robustness against a certain level of distortions caused by acceptable modifications. By comparing with two representative methods in the literature, this paper presents that the proposed method outperforms them with respect to discriminability and security. More importantly, an excellent tamper localization capability is demonstrated as well.

ACKNOWLEDGEMENTS

This work was funded by the German Research Foundation (DFG) as part of the research training group GRK 1564 'Image New Modalities'.

REFERENCES

Boncelet, C. (2006). The ntmac for authentication of noisy messages. *IEEE Trans. Inf. Forensics and Secur.*, 1(1):35–42.

Coskun, B. and Memon, N. (2006). Confusion/diffusion capabilities of some robust hash functions. In *Proc. Conf. Inf. Sci. and Syst.*, pages 1188–1193.

Dalal, N. and Triggs, B. (2005). Histograms of oriented gradients for human detection. In *Proc. IEEE Comput. Soc. Conf. on Comput. Vis. and Pattern Recognit.*, volume 1, pages 886–893.

Graveman, R. and Fu, K. (1999). Approximate message authentication codes. In *Proc. 3rd Annual Fedlab Symp. on Adv. Telecommun./Inf. Distrib.*

Han, S.-H. and Chu, C.-H. (2010). Content-based image authentication: current status, issues, and challenges. *Int. J. of Inf. Secur.*, 9(1):19–32.

Haouzia, A. and Noumeir, R. (2008). Methods for image authentication: a survey. *Multimed. Tools and Appl.*, 39(1):1–46.

Hsu, C.-Y., Lu, C.-S., and Pei, S.-C. (2009). Secure and robust sift. In *Proc. ACM Int. Conf. on Multimed.*, pages 637–640.

ISO/IEC9797 (2011). Information technology – security techniques – message authentication codes (macs).

Kozat, S., Venkatesan, R., and Mihcak, M. (2004). Robust perceptual image hashing via matrix invariants. In *Proc. IEEE Int. Conf. on Image Process.*, volume 5, pages 3443–3446.

Krawczyk, H. and Eronen, P. (2010). Hmac-based extract-and-expand key derivation function (hkdf). *RFC 5869*.

Lin, C.-Y. and Chang, S.-F. (2001). A robust image authentication method distinguishing jpeg compression from malicious manipulation. *IEEE Trans. Cir. and Sys. for Video Technol.*, 11(2):153–168.

Mihcak, M. K. and Venkatesan, R. (2001). New iterative geometric methods for robust perceptual image hashing. In *Revised Papers from the ACM CCS-8 Workshop on Secur. and Priv. in DRM 01*, pages 13–21.

Monga, V. and Evans, B. (2006). Perceptual image hashing via feature points: Performance evaluation and tradeoffs. *IEEE Trans. on Image Process.*, 15(11):3452–3465.

Nilsson, M., Dahl, M., and Claesson, I. (2005). The successive mean quantization transform. In *Proc. IEEE Int. Conf. on Acoust., Speech, and Signal Process.*, volume 4, pages 429–432.

NIST-FIPS (2013). Digital signature standard (dss). *Federal Information Processing Standards Publication (FIPS PUB) 186-4*.

NIST-SP (2009). Recommendation for key derivation using pseudorandom functions. *Special Publication 800-108*.

Queluz, M. (1998). Towards robust, content based techniques for image authentication. In *Proc. IEEE Int. Workshop on Multimed. Signal Process.*

Shin, J. and Ruland, C. (2013). A survey of image hashing technique for data authentication in wmsns. In *Proc. IEEE Int. Conf. on Wirel. and Mob. Comput., Netw. and Commun.*, pages 253–258.

Ur-Rehman, O. and Zivic, N. (2013). Fuzzy authentication algorithm with applications to error localization and correction of images. *WSEAS Trans. on Syst.*, 12:371–383.

Venkatesan, R., Koon, S.-M., Jakubowski, M. H., and Moulin, P. (2000). Robust image hashing. In *Proc. IEEE Int. Conf. on Image Process.*, volume 3, pages 664–666.

Xie, L., Arce, G., and Graveman, R. (2001). Approximate image message authentication codes. *IEEE Trans. on Multimed.*, 3(2):242–252.