Analysis of Perceptual Hashing System for Secure and Robust Image Hashing

Sahana M S[1], Veena S K[2]

[1] *PG Student, ECE Department, MIT, Karnataka, India*
[2] *Assistant Prof, ECE Department, MIT, Karnataka, India*

Abstract - ***Due to the popularity of digital technology, more and more digital images are being created and stored every day. Perceptual image hashing is conventionally used for content identification and authentication. In this paper, a theoretical analysis of perceptual hashing systems that use a quantization module followed by a crypto-compression module is proposed. Randomized feature extractions are made for security against intentional attacks and then finally image is encrypted using secret key Secure Hash Algorithm-1(256 bits).***

Key Words: *Feature extraction, Robust image hashing, Image authentication, Perceptual hashing.*

1. INTRODUCTION

Image Hash functions are also called message digest functions. Their purpose is to extract a short binary string from a large digital message. Complication arises when two images that appear identical to the human eye may have different digital representations. e.g. an original image and its compressed image.

To identify the changes in network and multimedia data, has gained more interest in developing more robust techniques and algorithms to check the authenticity, integrity and confidentiality. One possible way is to use of conventional cryptographic hashes such as secure hash algorithm 1 (SHA-1) [1].The main advantage of perceptual hashing schemes is that the multimedia data is not altered and not degraded at all.

In the literature, the technique used for network and multi-media verification can be classified into two categories: digital signature-based [2] and watermark-based [3]. Zhao et al. [4] proposed an approach for the combined image authentication and compression of images using a digital watermarking and data hiding technique.

An image hash algorithm proposed by Venkatesan et al [5] is developed based on an image statistics vector extracted from the various sub-bands in a wavelet decomposition of the image. The statistics such as averages of coarse sub-bands and variances of other (fine detail) sub-bands stay invariant under a large class of content-preserving modifications to the image but they do not necessarily capture content changes well, particularly those that are maliciously generated.

In [6] Lin and Chang have shown a mathematical invariant relationship between two discrete cosine transform (DCT) coefficients in a block pair before and after JPEG compression and selected it as the image feature.

Authors in [7] propose a perceptual hashing scheme based on a combination of the discrete wavelet transform (DWT) and the Radon transform. The algorithm can effectively detect malicious local changes, while also being robust against content-preserving modifications.

In [8] Diffie et al introduced the concept of public-key cryptography in order to solve the key management problem. In their concept, each person gets a pair of keys, one called the public key and the other called the private key. Each person's public key is published while the private key is kept secret. Secret key cryptography involves the use of one key. All keys in a secret-key cryptosystem must remain secret; secret-key cryptography often has difficulty providing secure key management, especially in open systems with a large number of users [9].

The authors in [10] [11] propose a histogram-based perceptual image hashing function using the resistance of two statistical features: image histogram in shape and mean value. However, the fragility to malicious attacks is a drawback. An improvement of this method is proposed in [12], where the authors propose an improved histogram-based image hashing scheme using a K-means algorithm, which obtains a better fragility result than in [11].
The common aspect between all of the above mentioned schemes is that they do not really take the crypto-compression stage into account. When the crypto compression stage is missed, security properties are threatened.

The aim of this paper is to develop a theoretical analysis of full perceptual hashing systems that use a quantization module followed by a crypto-compression module**.** Section 2, represents the proposed Methodology. In section 3, several experimental results are presented. Conclusions are drawn in Section 4.

2. PROPOSED METHODOLOGY

In this section a perceptual hashing scheme that is robust to the quantization stage is proposed. Based on the quantization problem in perceptual hashing systems, I propose to add new modules to the standard perceptual hashing system. The block diagram of the hash generation module is presented in Fig. 1. Various steps are involved in the hash generation process which is as follows:

1. Let the input image be represented by I of dimension N x M pixels. Image I is split in to non-overlapping blocks of dimension q x p pixels. This gives a total of (N/q) x (M/p) blocks. Each block is represented by , where i=1. . . (N/q) x (M/p).
2. Let $B_i(x_k, y_k)$ represent the gray value of a pixel at spatial location (x_k, y_k) in the block B_i, where k=1, . . . , x p. Let the mean of each block be represented by m_i, where i is the block index. Each m_i is calculated as follows:

$$m_i = \frac{1}{q \times p} \sum_{k=1}^{q \times p} B_i(x_k, y_k) \qquad (1)$$

All of the computed continuous means m_i present features extracted from the transformed image in the feature extraction stage. Thus, they should be quantized during the quantization stage to form the quantized intermediate perceptual hash vector with a specific quantization step Q. The uniform quantization technique is used in our scheme. Let m'_i be the element of the quantized intermediate perceptual hash vector of a specific index i. m'_i is calculated as follows:

$$m'_i = \frac{m_i}{Q} \times Q \qquad (2)$$

3. The sender determines the information about the desired robustness to the additive Gaussian noise, σ. Based on this information, the analysis module gives the appropriate percentage of the extracted features that must be selected for a chosen quantization step size and image block decomposition size. For the proposed method, the features are randomly selected taking into account the desired robustness.

4. The quantized intermediate perceptual hash vector is compressed and encrypted by the cryptographic hash function SHA-1.Consequently, the obtained final perceptual hash is 256 bits in size.

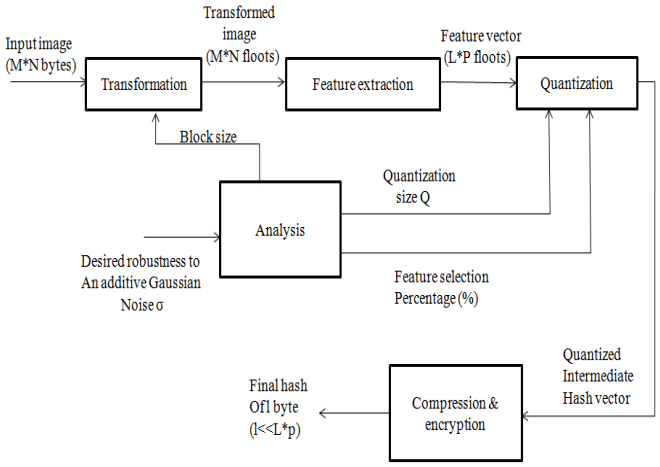

Fig -1: Proposed perceptual hashing scheme robust to the quantization stage.

3. RESULTS AND DISCUSSION

3.1 STRUCTURAL SIMILARITY EVALUATION

Fig. 2 shows an example of an original image and their noisy versions. An evaluation of the perceptual similarity between the original and the modified versions can be based on the perceptual aspect provided by the human visual system (HVS), on the method of the Structural Similarity (SSIM), or on the peak signal to noise ratio (PSNR) method which is as shown in Table. 1.

(a) (b)

(c) (d)

(e)

Fig-2: Original image and noisy versions with different additive Gaussian noise parameterized with different standard deviations σ: (a) original image, (b) σ=2 (c) σ= 4 (d) σ=20 (e) σ=35

Table -1: SSIM and PSNR values for noisy images obtained by applying different standard deviation values σ.

Standard deviation σ	SSIM	PSNR (dB)	Image quality	Perceptual hash
2	0.943	68.24	Very similar	$h(I_{ident})$
4	0.872	28.96	similar	$h(I_{ident})$
20	0.612	20.52	different	$h(I_{diff})$
35	0.248	14.37	Very different	$h(I_{diff})$

3.2 PRECISION-RECALL ANALYSIS

The precision-recall terminology comes from document retrieval where Recall measures how many correct documents were returned and precision quantifies how many of the returned documents are correct. Fig 3, 4, 5 compares my approach with others methods.

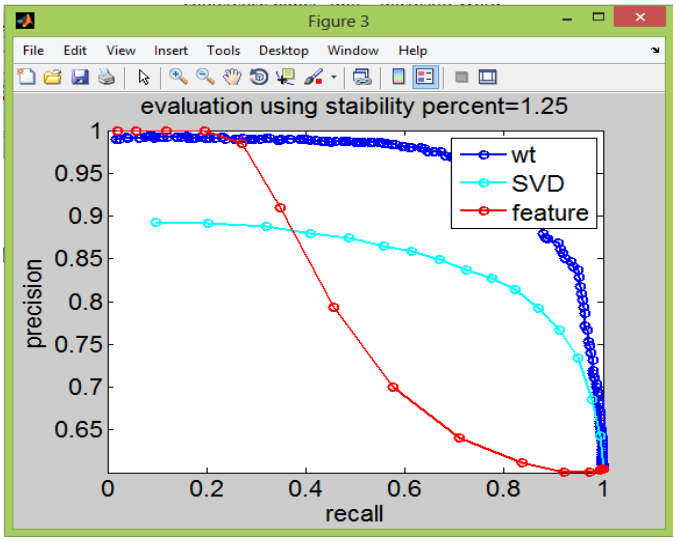

Fig -3: Precision-recall graph

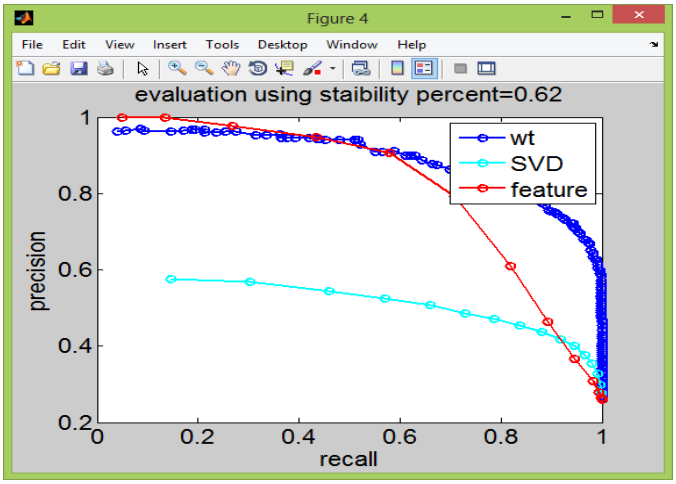

Fig -4: Precision-recall graph

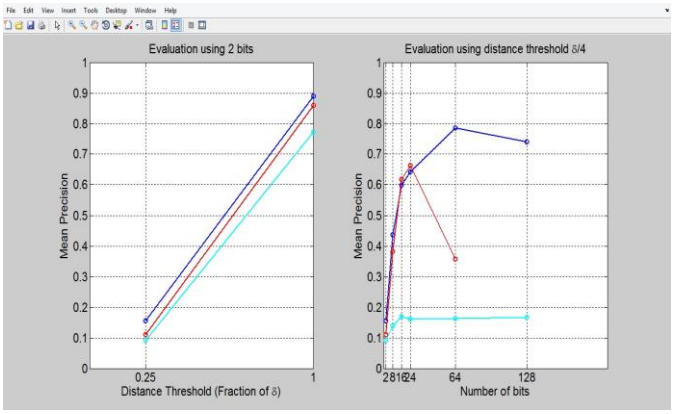

Fig -5: Comparision with other methods

3.3 ENCRYPTION STAGE

The encryption stage is the final step of perceptual hashing system which guarantees both system security and authentication.

Fig -6: Final encrypted image using secret key, which is known only to the intended user.

4. CONCLUSIONS

The Robustness, authentication, integrity and security are the most important requirements for a perceptual image hashing system. In this paper I have proposed a new perceptual hashing method that takes the quantization stage into account. Presented scheme is tested by several experiments to demonstrate the effectiveness of the proposed theoretical model and practical analysis for robust perceptual hashing.

ACKNOWLEDGEMENT

The authors would like to graciously thank Dr. B. G. Naresh Kumar, Principal and Dr Mahesh Rao, PG Coordinator, MIT, Mysore, for their extended support in project. Finally I would like to thank Veena S K, Assistant professor, MIT, Mysore, who has provided me with the best knowledge about the project.

REFERENCES

[1] Monjur Alam and Sonai Ray, "Design of an Intelligent SHA-1 Based Cryptographic System", International Journal of Network Security, Vol.15, No.6, PP.465-470, Nov. 2013

[2] C.-S. Lu and H.-Y. M. Liao, "Structural digital signature for image authentication", IEEE Trans. on Multimedia, vol. 5, pp. 161-173, June 2003.

[3] F. Khelifi, J. Jiang, "Perceptual image hashing based on virtual watermark detection", IEEE Transactions on Image Processing 19 (April) (2010) 981–994.

[4] Zhao, Y., Campisi, P. and Kundur, D., "Dual Domain Watermarking for Authentication and Compression of Cultural Heritage Images", IEEE Trans. on Image Processing, Vol. 13, pp.430-448, 2004.

[5] R. Venkatesan, S. M. Koon, M. H. Jakubowski, and P. Moulin, "Robust image hashing", Proc. IEEE Conf. on Image Processing, vol. 3, pp. 664-666, Sept. 2000

[6] Lin, C. Y. and Chang, S. F., "A Robust Image Authentication Method Distinguishing JPEG Compression from Malicious Manipulation", IEEE Trans. on Circuits and Systems of Video Technology, Vol. 11, pp.153 168, 2001 .

[7] X.C. Guo, D. Hatzinakos, "Content based image hashing via wavelet and Radon transform", in: Proceedings of the Multimedia 8th Pacific Rim Conference on Advances in Multimedia Information Processing, PCM'07,Springer-Verlag, Berlin, Heidelberg, 2007, pp. 755–764.

[8] W. Diffie and M. E. Hellman, (1976) "New Directions in Cryptography", IEEE Transactions on Information Theory, Vol. 22, No. 6.

[9] W. Diffie, (1988) "The First Ten Years of Public-Key Cryptography", Proceedings of the IEEE, Vol. 7#5, May 1988, pp. 560 - 577.

[10] S. Xiang, H.-J. Kim, J. Huang, "Histogram-based image hashing scheme robust against geometric deformations", in: Proceedings of the 9th Workshop on Multimedia & Security, ACM, New York, NY, USA, 2007, pp. 121–128.

[11] S. Xiang, H.-J. Kim, "Histogram-based image hashing for searching content-preserving copies", Transactions on Data Hiding and Multi- media Security 6 (2011) 83–108.

[12] Y. Ou, C. Sur, K. H. Rhee, "An improved histogram-based image hashing scheme using k-means segmentation", in: The Fourth Joint Work shop on Information Security (JWIS2009),Kaohsiung, Taiwan, August2009.

