A Review on Verifiable Image Licensing Approaches

Priyanshi Thakkar
Department of Computer Science and Engineering
Pandit Deendayal Energy University
Gandhinagar, India

Nishant Doshi
Department of Computer Science and Engineering
Pandit Deendayal Energy University
Gandhinagr, India

***Abstract*— Licensing an image refers to grant permission to use your image not to sell it full. Granting permission allows the person to edit, commerce and advertise usage also referred as the industry-standard method. Licensing the image allows to modify signing an agreement lays out the parameters, classification, and restrictions for utilizing an image. While techniques such as process of acme and perception ciphering can be used to verify the authenticity of an image and any modification specified in the contract, they are not able to determine who made the edits. Gradually gathering all the information of cryptographic. In past papers they have identified two key characteristics: 1. Authorized Use: Only a licensed individual or entity who follows the conditions outlined in a usage deal can create legitimate photos; 2. Productivity: validation of veritable image licensing system is fast and not affected by the number of edits or photos dimension.**

Keywords*— *Photograph usage rights, validatable photograph handling, secure cipher operations, digital authentications, two-way pairings.

I. INTRODUCTION

Photograph, a representation of the outside form of someone or element in artwork. every photograph has its personal copyrights that the writer or the individual that is publishing has given. If anyone who wants to edit or change the photo. Through public legislation, authorship rights are granted and infringement of those rights can result in penalties.

The copyright holder of a photograph can establish rules for its use by entering into a usage contract with the individual or entity seeking to use the photograph. Additionally to a payment, a standard licensing agreement includes three key elements: (a) the authenticity of the image, which includes identifying the authorship right owner, (b) the permitted user who has the right to operate the photograph and (c) the permissions granted for the image's use, including any restrictions or conditions on modifying the photo.

It is difficult for even experts to detect if a photograph has been altered using Photoshop if it is done intentionally. To prevent copyright infringement, technical solutions that match the photo licensing agreement are needed. There are various methods of authenticating photographs, such as watermarking, perception ciphering, and protected primitives. A digital watermark that is based on copyright protection is resistant to changes and provides a way to determine the originality of the photograph. The encoded information can be uncovered, even if the photograph has undergone changes. For example, A professional photograph with a "no-copy-allowed" watermark can resist typical image manipulations like JPEG compression, spinning, trimming, and adding disturbance. Watermarking is the process of embedding a digital code and is a well-established technique for identifying the source of a photograph without limiting the rights of the legal user or licensee.

Authenticating a photograph is the process of determining if the image has been tampered with and if it is genuine. Two common techniques for this are semi-fragile watermarks and perceptual ciphers. These methods help prevent editing of the image, but do not identify who made the changes.

II. LITERATURE

Traditional methods for authenticating photos, such as watermarking and perceptual hashinf, do not allow users to independently verify the validity of photos because these techniques require the help of the copyright holder.

VILS is different in that it allows for traceable image originality, assignable image editors and controllable editing behavior. An owner can give a unique code that allows access to their image and only authorized individuals can provide valid evidence of the image. Additionally, the image licensor can set rules for how much editing is allowed. One of the biggest advantages of VILS is that it allows for verifiable proof of the ownership, which has not been addressed by other photo authentication systems. Furthermore, it only allows certain key holders to edit the photo and takes into consideration the quality and size of the image.

Traditional methods of authenticating photographs include techniques like watermarking and perceptual hashing, which provide effective ways to verify the integrity of an image. Semi-fragile watermarks, which are embedded in pictures, can detect malicious attempts to alter the image but are still able to withstand benign changes that do not affect the actual content of the image. Researchers have proposed several promising approaches to this problem.

Traditionally, authenticating photographs has relied on techniques such as watermarking and perceptual ciphering, which are effective in verifying the originality of an image.

These semi-fragile watermarks embedded in images can detect any malicious changes made to the image, while remaining resilient to non-harmful changes that do not affect the image's content. Researchers have proposed various promising solutions to address this issue.

TABLE I. COMPARISON BETWEEN VILS AND OTHER CHANNELS

Primary	Permission Goal	Achievement				
		Protection	Strength	Permission	Capability	Load
SFW	Detail Verification	Disprovable	Yes	NO	>= O(N)	0
PHF	Detail Verification	Disprovable	Yes	NO	>= O(N)	O(1)
DSS	Ethics Identification	Verifiable	No	NO	O(1)	O(1)
DSS+CH	Random Cutting	Verifiable	Restricted	NO	O(N)	O(N)
DSS+CS	Acceptable Cutting	Verifiable	Restricted	NO	O(N)	O(1)
DSS+ACC	Detail Withdrawal	Verifiable	Restricted	NO	O(N)	O(1)
DSS+SNARKs	Confirmable photo modifying	Verifiable	Flexible	NO	>=O(N^2Log(N))	O(N)
DSS+ACC	Confirmable photo modifying	Verifiable	Flexible	NO	O(m)	O(1)
DSS+BLP	Confirmable and Acceptable photo modifying	Verifiable	Flexible	Yes	O(m)	O(1)

Perceptual hash: In this method of authenticating photographs, the image data is converted into a short sequence, known as a picture cipher, to confirm the reliability of the content. An photo cipher is a compressed illustration of an image created using a specific algorithm. The advantage of using image ciphering is that the cipher can be sent separately from the image. The purpose of perceptual ciphers is to create a unique "fingerprint" of an image for use in photo hunting and verifying photo information. Additionally, the cipher functions used in perceptual ciphering are designed to be robust to certain types of image manipulation. However, the image cipher cannot identify who made changes to an image and does not provide a way to identify the editor of an photo, similar to watermarking.

A. Cryptography-Based Image Authentication

The use of virtual autographs and absence of information proofs is increasing in picture verification. This method involves signing the picture information with a standard digital signature scheme (DSS) and sending the mark as a validation code to client along with the photo. The unforgeability feature of DSS ensures that no one, including users with good intentions, can alter retaining the photos validation code. Virtual marks can also be used to spot alteration as it is sensitive to changes. However, this approach for image identification may not be robust but it provides provable security and has limitations in detecting integrity issues.

B. Admissible Image Processing

Digital images are made up of two primary elements: snapshot parameters and snapshot message. Image data is the numerical values of the image's pixels stored in a computer, which sets computer generated images apart from printed ones. The image content, inversely, is the subject or meaning of the snapshot, which largely impacts its value in image-related applications. These operations allow users to achieve desired image content by editing the image data on a computer correctly.

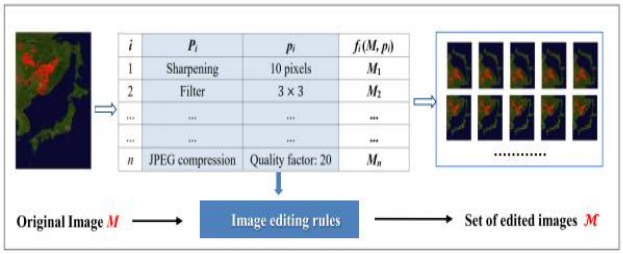

Fig. 1. The process algorithms

In this context, pi represents the specific processing parameters (such as a quality factor of 60) and n is the number of operations in P. For an image M, each operation results in a rare modified image Mi, represented as Mi = fi (M, pi). Approved image adjustment is defined as an method that processes an snapshot with modifications from set P, and outputs a set of photos M, denoted as M ← process (MP).

System Description:

A new image identification is developed by them keeping in mind following things:

1. Photo Copyright Holder (A licensor)
2. Legal Photograph Editor (a licensee)
3. Verifier

Security:

Safety is provided among competitor and an opponent. The attempts to compromise the scheme by working with the competitor. The security is ensured if the chances of the opponent successfully winning the game are minimal. This method of assessment, which typically involves a security reduction, is commonly employed in encryption-based process.

C. Experiment and Examination

a. Implementation and Evaluation of their system

In the practical implementation of a their system, Photoshop and similar software can be utilized to perform image manipulation procedures in an offline setting. As a result, the computational cost of the processing algorithm is not considered when evaluating this VILS. Consequently, the

efficiency of the cryptographic techniques employed plays a significant role in determining the effectiveness of our VILS.

b. Implementation and Testing

To assess performance more specifically, they carried out all the methods using the Synchronized Encrypted data bank. To test the performance of the scheme more intuitively, they chose a set of images from the Kotak image set3 for testing. The Kotak image set comprises of 28 lossless images, which they used to measure the effectiveness of system. VILS comprises of four tedious procedures: Key-Gen, Validate, Edit-Prove, and Confirm. In this test, the evaluating photos were converted into various forms from 200 to 2000 categories of processes for permission. In this process, the photos require to be pre-treated and Ciphered to a set before authorization. The binary data of each image is processed and reduced to a compact representation. Therefore, ciphering an photo obtains fewer than 1.5ms, this method proves to be far more efficient in comparison to conventional image processing techniques. It also shows that the most remarkable achievement is the constant overhead of verification time. The verification time remains constant at 19ms, regardless of the size of the image or the number of allowable operations. Cipher functions are utilized to transform photos of varying dimensions into fixed-size representations excluding duplication, and compression methods are employed to condense all cipher values into a concise and fixed-length validation code. As a result, the overhead for identification is consistent regardless of the photo dimension or count of processes. The VILS' adeptness testifies to its capability in providing efficient image licensing verification.

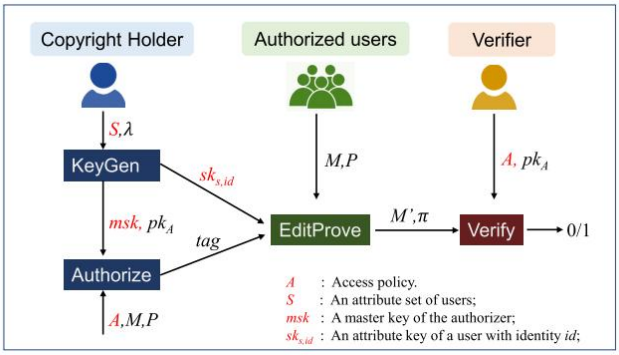

Fig. 2. Multi user image authorization

D. Scalability of multi person authorization

The VILS suggest scientific assistance for agreements between a photograph author (rights holder) and a permitted operator (permitted party). While it is created to certify photo processes for a one person at a time, it can be adapted to support multiple users by implementing principles of Ciphertext-policy attribute-based Encryption (CP-ABE). In CP-ABE, decoding keys are issued based on user's attributes and the data proprietor specifies an permission guidelines for the encryption text. By generating private keys of authorized users based on an attribute set S, the author (approver) can allow the photo(s) to many peoples with a protocols A on S. Those whose characteristics meets A can modify the photo with their identifier keys. A photo receiver checks an image based on A. Other developed techniques like context-aware seal, multi user seals, federation seal, secret splitting etc, can also be used as alternatives for creating image validation method when collaborative permission is needed.

III. ANALYSIS

From recent studies we can say that only one person can use it at one time, we need a system that provide multi user technology to save time and space. We can provide license on the image, that won't allow any third person to use our image which is called as trademark or say watermark. It also says if any person wants to crack the system or enters wrong password, the file will be automatically deleted. We also got information of how and what kind of attacks are seen on image.

TABLE. II COMPARISON OF SOME EXISTING SCHEMES

Snapshot dimension	Modification digits	Digit of entry	Time in seconds (s)			Memory (kB)	
			Origination	Validation	Affirmation	Size	Size of overhead
128*128	-----	12,531,999	~367	~306	~0.5	2.6*10^6	2.67
Unrestricted	1000	----	~1	0.33	~0.025	<13	<2
Unrestricted	1000	----	~1	0.35	~0.018	<15	<2

IV. CONCLUSION

A verifiable image licensing system (VILS) has been created by them as an efficient solution for authenticating the originality of an image, the valid client and the snapshot usage permission outlined in photo usage contracts. The system boasts advanced security features, such as tamper proofing and traceability, which greatly enhances its photo validation capabilities. Despite the increased number of elements to authenticate, the system's performance remains acceptable. The certifying process has a slight dip in performance, but the test process has seen a major upsurge of 40%. The team has come up with a design that enhances the VILS to include multi-user authorization utilizing the principles of Ciphertext-policy attribute-based Encryption (CP-ABE). They consider this approach as a possible solution for providing many people permission in cryptological-based photo identification plans.

REFERENCES

[1] Y. Yao, W. Zhang, H. Wang, H. Zhou, and N. Yu, "Content-adaptive reversible visible watermarking in encrypted images," Signal Process., vol. 164, pp. 386–401, Nov. 2019.

[2] H. M. Al-Otum, "Semi-fragile watermarking for grayscale image authentication and tamper detection based on an adjusted expanded-bit multiscale quantization-based technique," J. Vis. Commun. Image Represent., vol. 25, no. 5, pp. 1064–1081, Jul. 2014.

[3] J. Serra-Ruiz, A. Qureshi, and D. Megías, "Entropy-based semi-fragile watermarking of remote sensing images in the wavelet domain," Entropy, vol. 21, no. 9, p. 847, Aug. 2019.

[4] F. Peng, Z.-X. Lin, X. Zhang, and M. Long, "A semi-fragile reversible watermarking for authenticating 2D engineering graphics based on improved region nesting," IEEE Trans. Circuits Syst. Video Technol., vol. 31, no. 1, pp. 411–424, Jan. 2021.

[5] A. Egorova and V. Fedoseev, "Semi-fragile watermarking for JPEG image licensing Process - Google Search,

https://www.google.com/search?client=firefox-b-d&q=what+is+image+licensing

[6] A. Zhuvikin, V. I. Korzhik, and G. Morales-Luna, "Semi-fragile image authentication based on CFD and 3-bit quantization," CoRR, vol. abs/1608.02291, 2016.

[7] D.-C. Lou and J.-L. Liu, "Fault resilient and compression tolerant digital signature for image authentication," IEEE Trans. Consum. Electron., vol. 46, no. 1, pp. 31–39, Feb. 2000.

[8] Q. Sun and S.-F. Chang, "A robust and secure media signature scheme for JPEG images," J. VLSI Signal Process. Syst. Signal, Image Video Technol., vol. 41, no. 3, pp. 305–317, Nov. 2005.

[9] E. Kee, M. K. Johnson, and H. Farid, "Digital image authentication from JPEG headers," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 1066–1075, Sep. 2011.

[10] K. Iida and H. Kiya, "Robust image identification for double-compressed and resized JPEG images," in Proc. Asia–Pacific Signal Inf. Process. Assoc. Annu. Summit Conf. (APSIPA ASC), Honolulu, HI, USA, Nov. 2018, pp. 1968–1974.

[11] H. Yao, H. Wei, C. Qin, and X. Zhang, "An improved first quantization matrix estimation for nonaligned double compressed JPEG images," Signal Process., vol. 170, May 2020, Art. no. 107430.

[12] A. Sivaminathan, Y. Mao, and M. Wu, "Image hashing resilient to geometric and filtering operations," in Proc. IEEE 6th Workshop Multimedia Signal Process., Jun. 2004, pp. 355–358.

[13] A. Swaminathan, Y. Mao, and M. Wu, "Robust and secure image hashing," IEEE Trans. Inf. Forensics Security, vol. 1, no. 2, pp. 215–230, Jun. 2006.

[14] R. Davarzani, S. Mozaffari, and K. Yaghmaie, "Perceptual image Ciphering using center-symmetric local binary patterns," Multimedia Tools Appl., vol. 75, no. 8, pp. 4639–4667, Apr. 2016.]

[15] S. Pramanik, S. K. Bandyopadhyay, and R. Ghosh, "Signature image hiding in color image using steganography and cryptography based on digital signature concepts," in Proc. 2nd Int. Conf. Innov. Mech. Ind. Appl. (ICIMIA), Mar. 2020, pp. 665–669.

[16] A. Swaminathan, Y. Mao, and M. Wu, "Robust and secure image Ciphering," IEEE Trans. Inf. Forensics Security, vol. 1, no. 2, pp. 215–230, Jun. 2006.

[17] R. Davarzani, S. Mozaffari, and K. Yaghmaie, "Perceptual image Ciphering using center-symmetric local binary patterns," Multimedia Tool Appl., vol. 75, no. 8, pp. 4639–4667, Apr. 2016.

[18] Z. Tang, X. Zhang, X. Li, and S. Zhang, "Robust image Ciphering with ring partition and invariant vector distance," IEEE Trans. Inf. Forensics Security, vol. 11, no. 1, pp. 200–214, Jan. 2016.

[19] G. L. Friedman, "The trustworthy digital camera: Restoring credibility to the photographic image," IEEE Trans. Consum. Electron., vol. 39, no. 4, pp. 905–910, Nov. 1993.

[20] J. Kim, S. Lee, J. Yoon, H. Ko, S. Kim, and H. Oh, "PASS: Privacy aware secure signature scheme for surveillance systems," in Proc. 14th IEEE Int. Conf. Adv. Video Signal Based Surveill. (AVSS), Lecce, Italy, Aug. 2017, pp. 1–6.

[21] H. Chen, S. Wang, H. Zhang, and W. Wu, "Image authentication for permissible cropping," in Proc. 14th Int. Conf. Inscrypt, Fuzhou, China, Dec. 2018, pp. 308–325.

[22] H. Chen, X. Huang, W. Wu, and Y. Mu, "Privacy-aware image authentication from cryptographic primitives," Comput. J., vol. 64, no. 8, pp. 1178–1192, Aug. 2021.

[23] A. Naveh and E. Tromer, "PhotoProof: Cryptographic image authentication for any set of permissible transformations," in Proc. IEEE Symp. Secure Privacy (SP), San Jose, CA, USA, May 2016, pp. 255–271.

[24] D. Pointcheval and J. Stern, "Security proofs for signature schemes," in Proc. Int. Conf. Theory Appl. Cryptograph. Techn., vol. 1070. Zaragoza, Spain: Springer, May 1996, pp. 387–398.

[25] N. Bari´c and B. Pfitzmann, "Collision-free accumulators and fail-stop signature schemes without trees," in Proc. Int. Conf. Theory Appl. Cryptograph. Techn. Berlin, Germany: Springer, 1997, pp. 480–494.

[26] X. Chen, F. Zhang, and K. Kim, "Chameleon hashing without key exposure," in Proc. 7th Int. Conf. ISC, Palo Alto, CA, USA, Sep. 2004, pp. 87–98.C.

[27] G. Ateniese and B. de Medeiros, "On the key exposure problem inchameleon hashes," in Proc. 4th Int. Conf. SCN, Amalfi, Italy, Sep. 2004, pp. 165–179.

[28] S. A. Shah, I. A. Khan, S. Z. H. Kazmi, and F. H. B. M. Nasaruddin,"Semi-fragile watermarking scheme for relational database tamper detection," Malaysian J. Comput. Sci., vol. 34, no. 1, pp. 1–12, 2021..

[29] P. Lefèvre, P. Carré, C. Fontaine, P. Gaborit, and J. Huang, "Efficient image tampering localization using semi-fragile watermarking and error control codes," Signal Process., vol. 190, Jan. 2022, Art. no. 108342.

[30] L. Du, A. T. S. Ho, and R. Cong, "Perceptual hashing for imageauthentication: A survey," Signal Process., Image Commun., vol. 81, Feb. 2020, Art. no. 115713.

[31] Z. Su, L. Yao, J. Mei, L. Zhou, and W. Li, "Learning to hash for personalized image authentication," IEEE Trans. Circuits Syst. Video Technol., vol. 31, no. 4, pp. 1648–1660, Apr. 2021.

[32] R. Biswas, V. González-Castro, E. Fidalgo, and E. Alegre, "A new perceptual hashing method for verification and identity classification of occluded faces," Image Vis. Comput., vol. 113, Sep. 2021, Art. no. 104245.

[33] V. Monga and B. L. Evans, "Perceptual image hashing via feature points: Performance evaluation and tradeoffs," IEEE Trans. Image Process., vol. 15, no. 11, pp. 3452–3465, Nov. 2006.

[34] S. Xiang, H.-J. Kim, and J. Huang, "Histogram-based image hashing scheme robust against geometric deformations," in Proc. 9th Workshop Multimedia Secur. (MM Sec), Dallas, TX, USA, 2007, pp. 121–128.

[35] Y. S. Choi and J. H. Park, "Image hash generation method using hierarchical histogram," Multimedia Tools Appl., vol. 61, no. 1, pp. 181–194, Nov. 2012.

[36] C.-Y. Lin and S.-F. Chang, "A robust image authentication method distinguishing JPEG compression from malicious manipulation," IEEE Trans. Circuits Syst. Video Technol., vol. 11, no. 2, pp. 153–168, Feb. 2001

[37] S. Khan, "CLIFD: A novel image forgery detection technique using digital signatures," J. Eng. Res., vol. 9, no. 1, pp. 168–175, 2021. E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza, "Succinct noninteractive arguments for a von Neumann architecture," IACR Cryptol. ePrint Arch., vol. 2013, p. 879, Dec. 2013.

[38] S. Pramanik, S. K. Bandyopadhyay, and R. Ghosh, "Signature image hiding in color image using steganography and cryptography based on digital signature concepts," in Proc. 2nd Int. Conf. Innov. Mech. Ind. Appl. (ICIMIA), Mar. 2020, pp. 665–669.

[39] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil

[40] Pairing," in Proc. 7th Int. Conf. Theory Appl. Cryptol. Inf. Secur., in

[41] Lecture Notes in Computer Science, vol. 2248, C. Boyd, Ed. Gold Coast, QLD, Australia, Dec. 2001, pp. 514–532.

[42] L. Nguyen, "Accumulators from bilinear pairings and applications,"in Proc. Cryptographers Track RSA Conf., San Francisco, CA, USA, Feb. 2005, pp. 275–292.

[43] F. Guo, W. Susilo, and Y. Mu, Introduction to Security Reduction. Berlin, Germany: Springer, 2018.

[44] J. Ning, Z. Cao, X. Dong, L. Wei, and X. Lin, "Large universe ciphertext-policy attribute-based encryption with white-box traceability,"in Proc. Eur. Symp. Res. Comput. Secur. Cham, Switzerland: Springer, 2014, pp. 55–72..

[45] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. 13th ACM Conf. Comput. Commun. Secur., 2006, pp. 89–98.

[46] H. K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-based signatures," in Proc. Cryptographers Track RSA Conf. Berlin, Germany: Springer, 2011, pp. 376–392.

[47] J. Ning, Z. Cao, X. Dong, K. Liang, H. Ma, and L. Wei, "Auditable σ-time outsourced attribute-based encryption for access control in cloud computing," IEEE Trans. Inf. Forensics Security, vol. 13, no. 1, pp. 94–105, Jan. 2018.

[48] J. Ning, X. Huang, W. Susilo, K. Liang, X. Liu, and Y. Zhang, "Dual access control for cloud-based data storage and sharing," IEEE Trans. Depend. Sec. Comput., vol. 19, no. 2, pp. 1036–1048, Mar./Apr. 2022, doi: 10.1109/TDSC.2020.3011525.

[49] M. Bellare and G. Fuchsbauer, "Policy-based signatures," in Proc. Int. Workshop Public Key Cryptogr. Berlin, Germany: Springer, 2014, pp. 520–537.

[50] D. Boneh, X. Boyen, and H. Shacham, “Short group signatures,” in Proc. Annu. Int. Cryptol. Conf. Berlin, Germany: Springer, 2004, pp. 41–55.

[51] D. Chaum and E. Van Heyst, “Group signatures,” in Proc. Workshop Theory Appl. Cryptograph. Techn. Berlin, Germany: Springer, 1991, pp. 257–265.

[52] A. Bender, J. Katz, and R. Morselli, “Ring signatures: Stronger definitions, and constructions without random oracles,” in Proc. Theory Cryptogr. Conf. Berlin, Germany: Springer, 2006, pp. 60–79.

[53] E. Karnin, J. Greene, and M. Hellman, “On secret sharing systems,”IEEE Trans. Inf. Theory, vol. IT-29, no. 1, pp. 35–41, Jan. 1983.