The multimedia blockchain: a distributed and tamper-proof media transaction framework

BHOWMIK, Deepayan <http://orcid.org/0000-0003-1762-1578> and FENG, Tian

Published version

BHOWMIK, Deepayan and FENG, Tian (2017). The multimedia blockchain: a distributed and tamper-proof media transaction framework. In: Digital Signal Processing (DSP), 2017 22nd International Conference on, London, 2017-August, 3 November 2017. IEEE.

The Multimedia Blockchain: A Distributed and Tamper-Proof Media Transaction Framework

Deepayan Bhowmik* and Tian Feng†
*Department of Computing, Sheffield Hallam University, Sheffield, United Kingdom, S1 1WB
†Dept. of Electrical & Electronic Engineering, The University of Sheffield, Sheffield, United Kingdom, S1 4DE
deepayan.bhowmik@shu.ac.uk and t.feng@sheffield.ac.uk

***Abstract*—A distributed and tamper proof media transaction framework is proposed based on the blockchain model. Current multimedia distribution does not preserve self-retrievable information of transaction trails or content modification histories. For example, digital copies of valuable artworks, creative media and entertainment contents are distributed for various purposes including exhibitions, gallery collections or in media production workflow. Original media is often edited for creative content preparation or tampered with to fabricate false propaganda over social media. However there is no existing trusted mechanism that can easily retrieve either the transaction trails or the modification histories. We propose a novel watermarking based Multimedia Blockchain framework that can address such issues. The unique watermark information contains two pieces of information: a) a cryptographic hash that contains transaction histories (blockchain transactions log) and b) an image hash that preserves retrievable original media content. Once the watermark is extracted, first part of the watermark is passed to a distributed ledger to retrieve the historical transaction trail and the latter part is used to identify the edited / tampered regions. The paper outlines the requirements, the challenges and demonstrates the proof of this concept.**

I. Introduction

Media distribution also referred as content delivery is a form of digital distribution of multimedia contents which include audio, image and video. Historically the media distribution relied on physical exchange of papers, compact discs, DVDs or magnetic tapes. However online delivery medium such as the Internet based cloud services [1] or peer-to-peer communication is now the de-facto standard for multimedia delivery ensuring high availability, high performance and cost effectiveness. A content distribution network (CDN) is a distributed network of specialized servers optimised for seamless delivery of rich media to internet-connected devices. Cloud-based CDNs are preferred over traditional CDNs due to cost efficient hosting services without owning infrastructure.

Significant effort were made in the research as well as in the industry for efficient multimedia distribution systems. For example the MPEG Media Transport standard was developed as part of MPEG for multimedia delivery over the Internet which aimed at content-centric networking for more efficient content distribution through the network [2]. A new method of generating, distributing and using the multimedia file was proposed by indexing multiple video, audio, subtitle tracks and metadata within the media file [3]. However, none of these solutions focuses on the security and integrity of the delivered content, *e.g.*, indexes can be easily removed from the content loosing the track of the associated information.

Zhou *et al.* [4] proposed a joint physical and application layer security framework that exploits the security capacity and signal processing techniques at the physical layer; and the authentication and watermarking techniques at the application layer. The scheme aimed at secure delivery of multimedia packets over wireless network and did not consider any integrity of the media in case of tampering. Further multimedia content protection techniques were proposed using secure watermarking [5] and joint compression and encryption [6] based approaches. However, both the algorithms focused only on content protection without any discussion on how these techniques can be integrated within a media distribution framework.

In this paper we propose a novel distributed and tamper proof media transaction framework based on blockchain architecture. Blockchain is a relatively new and promising technology that has the potential to introduce transparency and trust to openly protect a network and validate transactions [7]. Current multimedia distribution does not preserve self-retrievable information of transaction trails or content modification histories. For example, digital copies of valuable artworks, creative media and digital archives (e.g., books) are distributed for various purposes including exhibitions, library archival or gallery collections. In another scenario, original media (document, image or video) is often edited for creative content preparation or tampered with to fabricate false propaganda over social media.

In absences of an existing trusted mechanism that can easily retrieve either the transaction trails or the modification histories, we propose a novel watermarking based Multimedia Blockchain framework that can address such issues. The unique watermark information contains two pieces of information: a) a hash containing transaction histories (blockchain transactions log) and b) an image signature preserving retrievable original media content. Once the watermark is extracted, the former segment is passed to a distributed ledger that can retrieve the historical trail and the latter part is used to locate and reconstruct the edited/tampered regions. The reconstruction of the original content is achieved by finding an optimal solution using a compressive sensing algorithm. This paper outlines the requirements, the challenges and demonstrates the proof of the concept.

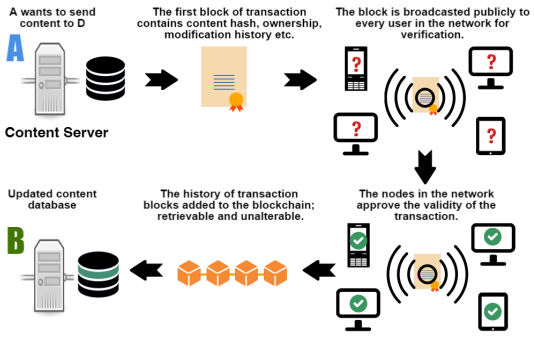

Fig. 1. Overview of the blockchain working principle.

II. Background

A. Blockchain

Blockchain [7] is an emerging technology and is essentially an open distributed *ledger* (database) that records all transactional details referred as *blocks*. Each record or block is timestamped and linked to a previous block and resilient to modification of the data and hence considered to be trusted for transactions between two entities in an efficient, verifiable and permanent way. Increasing investments in this technology were noticed in recent years from many large banks, financial institutions and other companies that intend to adopt the concept to provide a secure and publicly verifiable transaction mechanism. For example, Bitcoin[1], a recent disruptive digital currency, uses blockchain as its core technology.

BlockChain technology falls under the domain of distributed ledger technology allowing transactions to function in a decentralised way, *i.e.*, allows transactions to be verified without using a central organisation to process the transaction [8]. Instead multiple nodes are used to form a consensus on whether a transaction is valid or not. An example of blockchain working principle is shown in Fig. 1 where a payment is sent from A to B while other nodes verify the transaction. In case of a transaction failure or invalidation, the transaction is not acknowledged. Eventually all nodes will verify and add the transaction to their copy of the ledger. Conceptually it works by connecting or chaining blocks of information about the transactions and storing them together in a chronological order and hence called *blockchain*.

Beyond digital currency, this technology has major potential usage in transferring any digital content. Current other potential application scenarios include hardware and software wallets, compliance and identity and a number of other financial and transaction management applications, such as *smart contracts* [9]. Essentially blockchain is relevant to anything that requires transaction verification or a signature [7] leading to authenticity and trust. However, no major effort was noticed in multimedia applications except a basic blockchain based digital rights management concept introduced by Fujimura *et al.* [10] where the right information was added as part of blockchain transaction. On contrary in this work we propose a complete framework that keeps all records of the media transactions (*e.g.*, ownership, licenses etc.) as well as offers mechanism for tamper-proof verifiable integrity of the media enhancing trust among stakeholders.

[1]https://bitcoin.org/

B. Multimedia Security

As digital technologies have shown a rapid growth within the last decade, content protection now plays a major role within content management systems. Of the current systems, digital watermarking provides a robust and maintainable solution to enhance media security. Evidence of popularity of watermarking is clearly visible in the literature where majority of the papers penned their motivation for media copyright protection and proposed watermarking algorithms that are either imperceptible [11], robust against various intentional [12] and unintentional (*e.g.*, compression [13], filtering [14] or geometric [15]) attacks, fragile [16] or secure [5]. A self-embedding watermarking scheme [17] essentially embeds the host image information as watermark within the image itself. Such schemes allow tamper detection and recovery of the original image.

Cox *et al.* [18] listed various applications of watermarking including *broadcast monitoring*, *owner identification*, *proof of ownership*, *authentication*, *transactional watermarking*, *copy control* and *covert communication*. A image quality evaluation method was proposed where a watermark is embedded using the discrete wavelet transform (DWT) [19] and the degradation of the extracted watermark was used to determine the quality without any reference to the original image. Yamada *et al.* [20] developed a real-time watermarking system for video-on-demand services where frame images are watermarked, unique to the user, when a server receives request from a user. The system aims to deter piracy.

With the motivation to propose a distributed and tamper-proof media transaction framework, our approach combines the concepts of blockchain and self embedding watermarking. While the blockchain offers a trusted mechanism for distributed content transaction framework, a frequency domain wavelet based self-embedding watermarking algorithm ensures content integrity by detecting and recovering any tampering/editing attempt on the host media.

III. Proposed Framework

The proposed distributed and tamper proof media transaction framework based on blockchain model consists of three parts: *a)* a Compressed Sensing (CS) based self-embedding watermarking, *b)* a Blockchain distributed ledger and *c)* authentication. The framework is depicted in Fig. 2 showing content preprocessing (for self-embedding watermarking) and registration in the blockchain and in Fig. 3 describing the content authentication workflow.

A. Self-embedding watermarking

A *self-embedding* watermarking scheme is intended to carry the information to authenticate an image which can be used to identify the counterfeit regions of the tampered image [17].

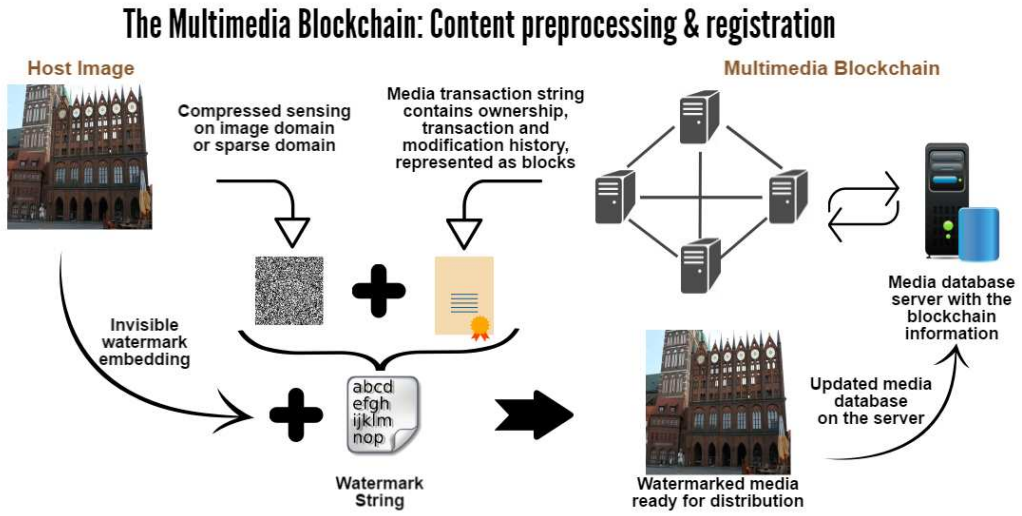

Fig. 2. Overview of the proposed multimedia blockchain framework: content processing and transaction.

Valensize *et al.* [21] proposed a compressive sensing based watermarking scheme for tampering detection. Motivated by early successes in the recent literature, we propose a compressive sensing based self-embedding watermarking algorithm in the context of our proposed *Multimedia Blockchain* framework. Our algorithm uses a pseudo-random projection (on a down sampled version) of the original image as the watermark and embeds it robustly within the host using a wavelet based technique. Once extracted the host image is recovered using a compressive sensing base image reconstruction algorithm.

1) Watermarking: Recently frequency domain watermarking techniques particularly wavelet based techniques have shown better promises in balancing imperceptibility and robustness [11], [13]. In this work we have used a wavelet based watermark embedding scheme where the low frequency coefficients are modified according to the watermark information. *a)* Firstly the watermark is constructed using CS-based pseudo-random projection of the down-sampled original image (as shown in Fig. 2). This is then combined with other blockchain transaction information to form the watermark character string. The length of the string depends on the image dimensions as well as the blockchain transaction. In our experimental set up we used a 8220 $(8154 + 66)$ byte long watermark string for an image size of 3264×2448. *b)* A one level 5/3 lifting based wavelet transform is then applied to the original image and low frequency subband (LL) coefficients are used to embed the watermark. The watermark bytes are spawned to form a single binary string and each bits are embedded by adjusting two adjacent coefficients, *i.e.*, one should be greater than the other to embed 1 and vice a versa for 0. The string is embedded repeatedly throughout the subband ensuring robust watermark extraction in the event of tampering. *c)* Finally during authentication the extracted watermarks are passed to the CS based sparse reconstruction module (as described below) to retrieve the original image. A comparison between the received image and the retrieved image helps to identify region of tampering and recover the original content. Brief details of the CS based reconstruction is given below.

2) Signal Recovery using Compressed Sensing: The CS theory proved that it is possible to reconstruct a signal with sparse representation from a reduced set of linear measurements compared to the minimum sampling-rate of Shannon-Nyquist theorem. The standard CS model for a given signal $x \in \mathbb{R}^n$ in the sparse domain can be described as:

$$y = \mathbf{\Phi} x \tag{1}$$

where $\mathbf{\Phi}$ is the sensing matrix with $m \times n, m \ll n$ & $y \in \mathbb{R}^m$.

The sparse signal is consisted of small number of non-zero coefficients. Hence, the dense image I usually required a sparsifying transform *e.g.*, DFT, DCT or DWT with basis functions $\mathbf{\Psi}$ to achieve a more compact energy distribution of the signal [21].

$$x = \mathbf{\Psi} I \tag{2}$$

The reconstruction operation is usually a non-linear operation to reconstruct an approximation of the original signal. Since the optimization constraints of reconstructions are different, some algorithms can reconstruct the image domain values without sparsifying the transform in Eq. (2). The self-embedded watermark of image hash based on CS is produced as follows:

- Image I is down sampled to a lower resolution $(N \times M)$ to ensure a realistic CS problem.
- The down sampled image I_d is then randomly sampled by $\mathbf{\Phi}$ directly, or the transform coefficients x_d of I_d are random sampled by $\mathbf{\Phi}$.
- The randomly sampled values y in image domain or transform coefficients in the frequency domain are stored as the image hash watermark w.

The extracted watermark w' from tampered image can be seen as the compressed samples y' to reconstruct the down sampled original image I_d. Then, the tampering detection can

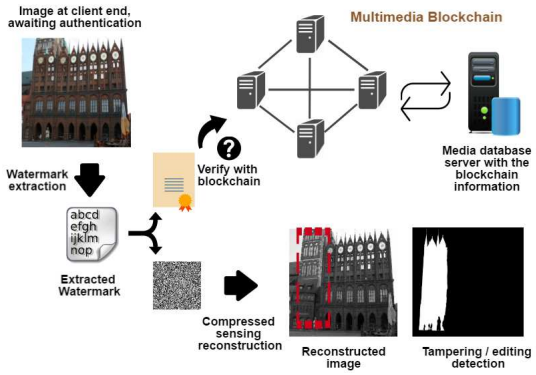

Fig. 3. Functional block diagram of content authentication and reconstruction.

be applied. The proposed scheme is flexible to various CS methods. In particular, two recovery strategies were tested:

- Minimization of the $l1$-*norm* of the images DWT coefficients and
- Minimization of the images Total-Variation norm [22].

B. The Multimedia Blockchain

The proposed framework uses a standard blockchain infrastructure and was amended to satisfy the requirements of the multimedia blockchain. As shown in Fig. 2 and Fig. 3, the frame contains two parts: 1) content preprocessing (for self-embedding watermarking) and registration within the blockchain and 2) content authentication. The blockchain technology enables decentralized trustless digital transactions. Once the transaction is approved, the block is updated in the blockchain's permanent distributed ledger and recorded by every user in the network. The transaction can be embedded with smart contracts and the public information. This public information is useful to record the transaction information of the image/media *e.g.*, transaction and modification history, ownership, blockchain transaction ID etc. and the information of CS samples which can be used to reconstruct the original image/media. This public information is embedded within the image/media itself before distribution. Once the transaction is approved, the image/media is ready to distribute and stored in a linked content server (*media database server* in Fig. 2). Corresponding blockchain information of transacted image/media in the database server is updated.

Further distribution or authentication is realized by extracting the watermark of the query image/media. The watermark of query image/media contains two parts: a blockchain transaction ID and the samples of original image for CS reconstruction. The former segment is passed to a distributed ledger that can retrieve the transaction detail and the latter part is used to reconstruct the original image/media and to locate the tampered regions, respectively. The blockchain transaction ID is used to retrieve the histories of the query image/media including the ownership information, sender's and receiver's address, time of the transaction, the block address of the transaction, price etc. (*e.g.*, Fig. 4). The CS samples are used to reconstruct the down sampled version of original image to identify any tampered or edited region with a possibility

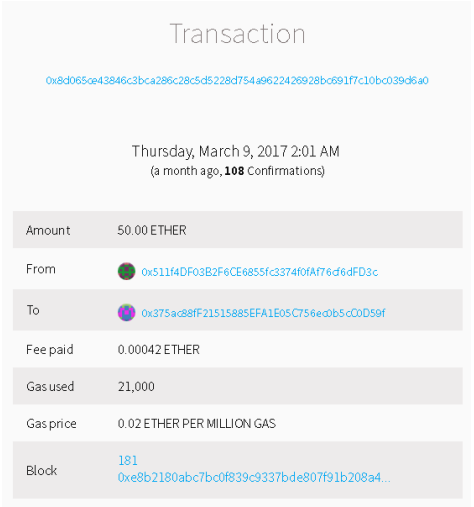

Fig. 4. The transaction history of a particular ID obtained using Ethereum.

Fig. 5. The image database.

to restore the original image region(s). If the blockchain verification or the tampering detection-authentication is failed, the query image/media is not authentic and it is not ready for further distribution / transaction.

IV. Results

For our framework, we have used an existing blockchain infrastructure. The blockchain network was build on the testnet of the Ethereum[2]. We also used an open source toolbox for the compressive sensing based sparse sample generation and reconstruction. The $l1-Magic$ [23] toolbox was used to solve both optimization problems, the wavelet basis was generated using the WAVELAB [24] package and the Noiselet basis of [25]. To emulate the tampering in content authentication, a standard dataset provided by Christlein *et al.* [26] was used.

In producing the results, firstly we generated transaction IDs through the Ethereum test-net and the sparse random samples from the host image. These two are concatenated to generate a watermarking string consists of a series of 8-bit values. Once watermarked, the image is tampered with existing tampering mask available from the benchmark dataset. Finally we extracted the watermark from this tampered image and reconstructed the original image in order to detect editing. A successfully tested example case is shown in Fig. 6 where (a) is the original image, (b) is the watermarked image, (c) is the tampered version, (d) is the reconstructed image using the extracted watermark and (e) is the detected tampered

[2]https://www.ethereum.org/

(a) (b) (c) (d) (e)

Fig. 6. (a) Original image (b) watermarked image (c) tampered image (d) reconstructed image using extracted watermark and (e) tampered region detection.

region. The extracted transaction ID was also retrieved to the corresponding transactions on the Ethereum test-net to authenticate the ownership and transaction history.

V. Conclusions

In this paper we proposed a new distributed and tamper proof media transaction framework based on the blockchain model. The proposed Multimedia Blockchain framework is built on a self-embedding watermarking algorithm that uses compressive sensing to detect any tampering and to retrieve the original content. We have successfully demonstrated the proof of this concept.

Acknowledgements

We acknowledge the support of the UK Engineering and Physical Research Council (EPSRC) through a researcher in residence fellowship at Digital Catapult, London.

References

[1] M. Hu, J. Luo, Y. Wang, and B. Veeravalli, "Practical resource provisioning and caching with dynamic resilience for cloud-based content distribution networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 8, pp. 2169–2179, Aug 2014.

[2] Y. Lim, K. Park, J. Y. Lee, S. Aoki, and G. Fernando, "MMT: An emerging MPEG standard for multimedia delivery over the internet," *IEEE MultiMedia*, vol. 20, no. 1, pp. 80–85, Jan 2013.

[3] A. U. A. A. Butt, S. R. Bramwell, and B. T. Fudge, "Multimedia distribution system," Jun. 25 2013, US Patent 8,472,792.

[4] L. Zhou, D. Wu, B. Zheng, and M. Guizani, "Joint physical-application layer security for wireless multimedia delivery," *IEEE Communications Magazine*, vol. 52, no. 3, pp. 66–72, March 2014.

[5] T. Bianchi and A. Piva, "Secure watermarking for multimedia content protection: A review of its benefits and open issues," *IEEE Signal Processing Magazine*, vol. 30, no. 2, pp. 87–96, March 2013.

[6] A. Pande, P. Mohapatra, and J. Zambreno, "Securing multimedia content using joint compression and encryption," *IEEE MultiMedia*, vol. 20, no. 4, pp. 50–61, Oct 2013.

[7] W. Mougayar, *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. John Wiley & Sons, 2016.

[8] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology? A systematic review," *PloS one*, vol. 11, no. 10, p. e0163477, 2016.

[9] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *Security and Privacy (SP), 2016 IEEE Symposium on*. IEEE, 2016, pp. 839–858.

[10] S. Fujimura, H. Watanabe, A. Nakadaira, T. Yamada, A. Akutsu, and J. J. Kishigami, "BRIGHT: A concept for a decentralized rights management system based on blockchain," in *IEEE 5th International Conference on Consumer Electronics - Berlin (ICCE-Berlin)*, 2015, pp. 345–346.

[11] D. Bhowmik, M. Oakes, and C. Abhayaratne, "Visual attention-based image watermarking," *IEEE Access*, vol. 4, pp. 8002–8018, 2016.

[12] M. Fallahpour, S. Shirmohammadi, M. Semsarzadeh, and J. Zhao, "Tampering detection in compressed digital video using watermarking," *IEEE Transactions on Instrumentation and Measurement*, vol. 63, no. 5, pp. 1057–1072, May 2014.

[13] D. Bhowmik and C. Abhayaratne, "Quality scalability aware watermarking for visual content," *IEEE Transactions on Image Processing*, vol. 25, no. 11, pp. 5158–5172, 2016.

[14] X. Zhu, J. Ding, H. Dong, K. Hu, and X. Zhang, "Normalized correlation-based quantization modulation for robust watermarking," *IEEE Trans. on Multimedia*, vol. 16, no. 7, pp. 1888–1904, Nov 2014.

[15] H. Zhang, H. Shu, G. Coatrieux, J. Zhu, Q. M. J. Wu, Y. Zhang, H. Zhu, and L. Luo, "Affine legendre moment invariants for image watermarking robust to geometric distortions," *IEEE Transactions on Image Processing*, vol. 20, no. 8, pp. 2189–2199, Aug 2011.

[16] H. T. Chan, W. J. Hwang, and C. J. Cheng, "Digital hologram authentication using a hadamard-based reversible fragile watermarking algorithm," *Journal of Display Technology*, vol. 11, no. 2, pp. 193–203, Feb 2015.

[17] D. Singh and S. K. Singh, "Effective self-embedding watermarking scheme for image tampered detection and localization with recovery capability," *Journal of Visual Communication and Image Representation*, vol. 38, pp. 775 – 789, 2016.

[18] I. J. Cox, M. L. Miller, and J. A. Bloom, "Watermarking applications and their properties," in *Information Technology: Coding and Computing, 2000. Proceedings. International Conference on*, 2000, pp. 6–10.

[19] S. Wang, D. Zheng, J. Zhao, W. J. Tam, and F. Speranza, "An image quality evaluation method based on digital watermarking," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 17, no. 1, pp. 98–105, Jan 2007.

[20] T. Yamada, M. Maeta, and F. Mizushima, "Video watermark application for embedding recipient id in real-time-encoding vod server," *Journal of Real-Time Image Processing*, vol. 11, no. 1, pp. 211–222, 2016.

[21] G. Valenzise, M. Tagliasacchi, S. Tubaro, G. Cancelli, and M. Barni, "A compressive-sensing based watermarking scheme for sparse image tampering identification," in *IEEE International Conference on Image Processing (ICIP)*, Nov 2009, pp. 1265–1268.

[22] L. I. Rudin, S. Osher, and E. Fatemi, "Nonlinear total variation based noise removal algorithms," *Physica D: Nonlinear Phenomena*, vol. 60, no. 1-4, pp. 259–268, 1992.

[23] E. Candes and J. Romberg, "l1-magic: Recovery of sparse signals via convex programming," *URL: www. acm. caltech. edu/l1magic/downloads/l1magic. pdf*, vol. 4, p. 14, 2005.

[24] J. B. Buckheit and D. L. Donoho, *Wavelab and reproducible research*. Springer.

[25] J. Romberg, "Imaging via compressive sampling," *IEEE Signal Processing Magazine*, vol. 25, no. 2, pp. 14–20, 2008.

[26] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6, pp. 1841–1854, Dec 2012.