VIJITH, V.A., GEORGE, A., AMBADIYIL, S., JHA, A.K. and PRABHU, R. 2024. Optimization of illumination for security hologram authentication. In *Bouma, H., Prabhu, R., Yitzhahy, Y. and Kuijf, H.J. (eds.) Advanced materials, biomaterials, and manufacturing technologies for security and defence II: proceedings of the 2024 SPIE Security + defence, 16-20 September 2024, Edinburgh, UK*. Proceedings of SPIE, 13206. Bellingham, WA: SPIE [online], paper 1320618. Available from: https://doi.org/10.1117/12.3034230

Optimization of illumination for security hologram authentication.

VIJITH, V.A., GEORGE, A., AMBADIYIL, S., JHA, A.K. and PRABHU, R.

2024

Optimization of Illumination for Security Hologram Authentication

Vijith V. A[1], Akhilesh George[1], Sajan Ambadiyil[2], Avinash Kumar Jha[3], Radhakrishna Prabhu[4]

[1] Department of Optoelectronics, University of Kerala, Thiruvananthapuram-695581, India,
[2] Center for Development of Imaging Technology, Thiruvananthapuram-695027, Kerala, India
[3] B2-1, Plaza Seren Acers, 200 feet road, Thoraipakkam, Chennai-600097, Tamil Nadu, India
[4] Robert Gordon University, School of Engineering, Aberdeen, United Kingdom

ABSTRACT

Security holograms, diffractive optical elements known for their intricate 3D visuals, are a cornerstone of brand protection. However, their effectiveness hinges on robust authentication methods. This work explores the critical role of illumination in hologram visualization for enhanced authentication. We investigate the impact of illumination angle and capture stage on the clarity of the hologram's visual features.

An experimental setup utilizing an LED light source, and a smartphone camera allows for systematic analysis of illumination angles. Laser light is also explored as a potential authentication tool. By combining observations, detailed documentation, and the potential of Artificial Intelligence (AI), this research aims to identify the optimal illumination conditions that maximize hologram visualization, facilitating efficient and reliable authentication workflows. This approach paves the way for improved security in document and product authentication, ultimately strengthening consumer trust and brand reputation.

Keywords: Hologram, Diffraction Efficiency, DOVID, Security, Authentication, Brand protection, Anti-counterfeit technology, Colour Temperature.

1. INTRODUCTION

Currently, various overt or covert brand protection solutions are available to ensure authenticity of products and safeguard against counterfeits [1-4]. Out of these, security holograms, also known as Diffractive Optically Variable Image Devices (DOVIDs), are widely employed on documents and packaging [5] to enhance the authenticity. Their intricate 3D visual effects, created using laser technology, shift dramatically with viewing angle, making them a valuable tool for product authentication. However, as counterfeiters gain access to advanced technologies, the need for more robust authentication methods grows.

Currently, there is no single, standardized method to definitively detect counterfeit holograms. This highlights the importance of a comprehensive approach to hologram authentication, starting with effective visualization. The critical challenge lies in the fact that the reflection patterns of holograms are highly sensitive to lighting conditions. A slight variation in illumination can significantly alter the visual representation of the hologram, potentially hindering authentication processes.

This research presents a novel investigation into optimizing illumination conditions for effective security hologram authentication. We explore the impact of both illumination angle and the capture stage on hologram visualization. Through a dedicated experimental setup utilizing an LED light source, a dimmer, a holder, and a smartphone camera module, we systematically analyse the effects of varying illumination angles. Additionally, we explore the potential of laser light in the authentication process.

Our study focuses on two key aspects: the optimal illumination angle for maximizing the clarity of the hologram and the ideal capture stage for further authentication processing. We leverage a combination of controlled observations, meticulous note-taking, and the potential of Artificial Intelligence (AI) to identify the optimal lighting conditions that facilitate superior hologram visualization, ultimately leading to more efficient authentication workflows.

This research aims to contribute to the ongoing effort to combat counterfeiting by establishing a foundation for optimized hologram illumination, ultimately enhancing the security of documents and products.

2. LITERATURE REVIEW

The security holograms are very sensitive to illumination due to their fabrication method. These holograms are based on the reflection and refraction of light so that they can only be visible in a certain intensity of illumination and angle.

In an earlier study by Hertog et. al., a combination of sunlight as well as artificial light was used illuminate the holograms and to enhance the image quality. They used a spectrophotometer to measure the spectral content and further analysed to extract the spectral components. They utilized a special algorithm to balance the colour temperature. However, the sun spectrum changes due to seasonal variations and changing sun's colour temperature were not accounted for [6]. In another work, Hyperspectral Imaging for mapping value of security hologram values such as reflectance and wavelength were studied. As per this study, wavelengths can affect the reflectance. They noticed that even a tiny change can significantly affect illumination and build-in quantity of source and handling setups [7]. The advanced technologies available in opto-electronics makes it simpler for the counterfeiters to access the information in a hologram and they reproduce a new hologram similar to it. Thus, the technologies need to be enhanced continuously to get rid of such forgeries. Techniques such as random phase encoding and correlation pattern recognition, watermark and stenographic marking, were investigated by many researchers in order to increase the difficulty in making fake holograms [8-11]. Cost effective hologram encoding schemes such as double exposure holographic interferometry in conjunction with random diffuser key hologram [12], using an encoded reference beam [13-16], artistic visualization of moire pattern produced by security and key hologram pairs [17-19] also have been reported for checking the authenticity of security holograms.

3. METHODOLOGY

This study investigates the optimal illumination conditions for effective visualization of security holograms, ultimately enhancing authentication processes. Our primary objective is to identify lighting conditions that maximize the clarity of the hologram's visual elements, enabling accurate processing for authentication.

The methodology employed a two-pronged approach:

3.1 Laser Light Exploration:

- An initial investigation utilized a helium-neon laser (Figure 3.1) to analyse diffraction patterns. The laser beam was directed at varying angles to observe the hologram's response.
- Diffraction efficiency was calculated based on observed measurements, but limitations arose due to:
  - Difficulty in clearly capturing the diffraction patterns for accurate measurement.
  - Inconsistent presence of diffraction patterns across different holograms.
  - Material properties influencing efficiency.

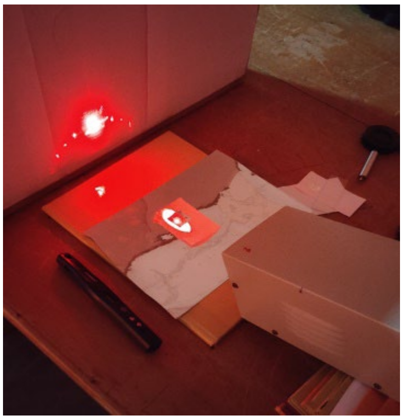

Fig.3.1 Laser Light Exploration

3.2 LED Illumination and Image Analysis:

- Following the laser experiment, we shifted to a white LED light source.
- Key light properties considered include:
  - **Colour Temperature:** Measured in Kelvin (K), it denotes the "warmth" or "coolness" of light (e.g., 2000K for warm yellow, 6500K for cool blue).
  - **Hue:** The perceived colour (red, green, blue, etc.).
  - **Value:** Lightness or darkness of a colour.
  - **Saturation:** The intensity or purity of a colour.
  - **Sharpness:** Clarity of details in an image.
- We aimed to identify the light intensity that yielded the best values for these parameters, ensuring optimal image capture for authentication processing.
- The experiment involved:
  - Utilizing LEDs with varying colour temperatures (6500K, 6000K, 5000K).
  - Setting the light source angle based on the optimal laser diffraction angle (if applicable).
  - Identifying the viewing angle that maximized visual clarity of the hologram's features.
  - Constructing a simple setup (Figure 3.2) with:
    - LED light source in a holder (20cm distance, 30° angle).
    - Smartphone camera positioned at the same distance (80° angle).
    - Dimmerstat to control light intensity.
  - Capturing images at various light intensities for multiple holograms.
- Image analysis employed Python programming to measure:
  - Saturation
  - Hue
  - Value
  - Sharpness
- The image exhibiting the highest sharpness value was considered optimal, indicating the most suitable illumination conditions for clear visualization.

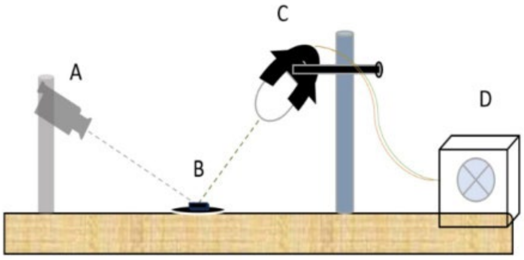

Fig.3.2. Experimental setup where A is the camera placed in a holder, B is the hologram to be illuminated, C is the illumination source (LED) fixed on a holder and D is the Dimmerstat for controlling light intensity

This methodology allowed us to systematically evaluate the impact of illumination on hologram visibility and identify the optimal lighting conditions for subsequent authentication processing through image analysis techniques.

4. RESULTS AND DISCUSSION

The captured images are utilised for programming using python. The program measures the parameters such as saturation, hue, value and contrast, which determines the quality of an image. The image quality is necessary in the stages of image processing for checking authentication of the said hologram. Although the hue, saturation and value measures had only a slight difference, the quality of the images could be determined by its sharpness. Higher the sharpness, better the images will be. From the program output, the sharpness of images were continuously increasing with the intensity change. But after a certain point, the sharpness was seen to be decreasing. It was found that the image had better sharpness when captured at 460 Lux (can vary between 450 –490 Lux). When the intensity was further increased, the sharpness keeps on decreasing. Figure 4.1 shows the sharpness at 460 Lux and at 500 Lux.

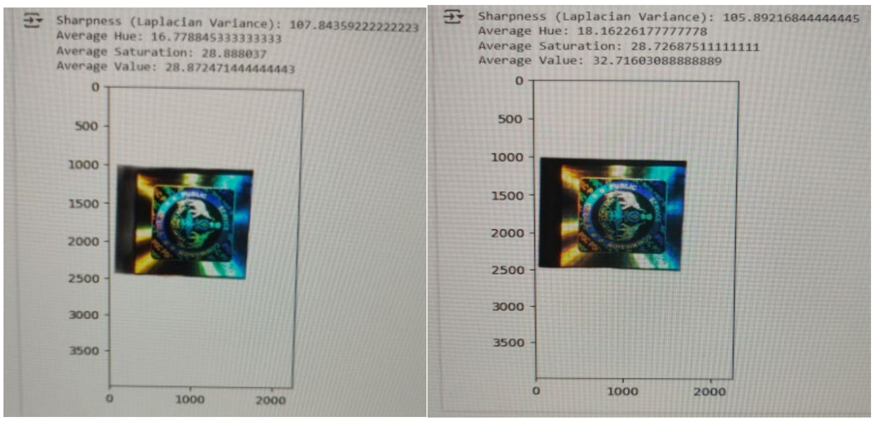

Fig. 4.1. Results from a hologram that was illuminated at 460 Lux (left) and at 500 Lux (right) respectively

The experiment was repeated using LEDs of different colour temperatures (6000K and 5000K). The observations showed that the sharpness lies below the optimum value that we got with that of 6500K. Thus, the image taken from an angle of 80^{o} and with the light angle of 30^{o} shows perfect illumination of hologram. The same was observed for different holograms as well, which is shown in Fig 4.2.

Fig 4.2 Two different holograms using the same illumination scheme

5. CONCLUSION

This research investigated the critical role of illumination in optimizing the visualization of security holograms for enhanced authentication workflows. We employed a two-step methodology: initial exploration with a laser light source followed by a more systematic analysis using LED illumination and image processing techniques.

The limitations encountered with laser light, such as difficulty in capturing clear diffraction patterns and material dependence, led us to adopt LED illumination. We explored the impact of key light properties like colour temperature on the captured image's quality. Our findings suggest that an illumination intensity between 450-490 Lux, achieved with an LED of approximately 6500K colour temperature, provides optimal conditions for capturing clear and sharp images of holograms. This, in turn, facilitates efficient image processing techniques crucial for robust hologram authentication.

By establishing a foundation for optimizing illumination conditions, this research contributes to strengthening security hologram effectiveness. The identified optimal lighting parameters pave the way for the development of reliable and efficient authentication methods, ultimately safeguarding brand reputation and consumer trust.

This study opens avenues for further exploration. Future research could investigate the integration of artificial intelligence based algorithms into the image analysis process for even more robust and automated hologram authentication. Additionally, exploring a wider range of LED colour temperatures and light source angles could provide further insights into optimizing illumination for various hologram types.

REFERENCES

[1] S Ambadiyil, R Jayarajan, V P M Pillai and R Prabhu, Feasibility Analysis of Unique ID (UID) Generation for Personal Authentication of Valuable Documents Using Dorsal Hand Vein Pattern, SPIE Security + Defence 2018, 10 - 14 September 2018, Berlin, https://doi.org/10.1117/12.2325346.
[2] Ross, G. A., Pollard, P., Hunter, C., Officer, S., Prabhu G. R ‘Optically detectable security feature’ US patent, 7129506, 2006
[3] Fluorescence lifetime assisted enhanced security feature in travel documents for border control and security applications, Radhakrishna Prabhu, Jincy Johny, Simon Officer, Wei Keung Fung, SPIE Security + Defence, Counterterrorism, Crime Fighting, Forensics, and Surveillance Technologies, 9 - 11 September 2019, Strasbourg, France. https://doi.org/10.1117/12.2535742

[4] S. Officer, R. Prabhu, P. Pollard, C. Hunter and G. Ross, Novel online optical security system based on rare earth doped micro glass beads, SPIE-IS&T conference on Electronic Imaging 2004, January 18-23, San Jose, CA, USA. DOI:10.1117/12.528191.

[5] S. Ambadiyil, K.G. Jayan, R Prabhu and V.P.M. Pillai, Microstructure encryption and decryption techniques in optical variable and invariable devices in printed documents for security and forensic applications, SPIE Optics + Optoelectronics, 13 - 16 April 2015 in Prague, Czech Republic. https://doi.org/10.1117/12.2179635.

[6] W. Hertog, A. Llenas, J. Carreras., Optimizing indoor illumination quality and Energy efficiency using a Spectrally tunable lighting system to augment natural daylight, Optics Express V23, I24, 2015, https://doi.org/10.1364/OE.23.0A1564

[7] Arvind Mukundan, Hsiang-Chen Wang, Yu-Ming Tsao., A Novel Multipurpose Snapshot Hyperspectral Imager used to Verify Security Hologram, IEEE Xplore, DOI: 10.1109/ICEET56468.2022.10007232.

[8] Wlodarczyk K.L., Ardron M., Weston N.J., Hand D.P., Holographic watermarks and stenographic markings for combating the counterfeiting practices of high-value metal products, Journal of Materials Processing Technology 264, 2019, pp.328-335, DOI: 10.1016/j.jmatprotec.2018.09.020.

[9] Refregier P., Javidi B., optical image encryption based on input plane and Fourier plane random encoding, Optics Letters 20(7), 1995, pp. 767-769, DOI: 10.1364/OL.20.000767

[10] Wang R.K., Watson I.A., Chatwin C.R., Random phase encoding for optical security, optical Engineering 35(9), 1996, p.2464, DOI: 10.1117/1.600849.

[11] Zlokazov E.Yu., Starikov R.S., Odinokov S.B., Tsyganov I.K., Talalaev V.E., Koluchkin V.V., Specificity of correlation pattern recognition methods application in security holograms identity control apparatus, Physics Procedia 73, 2015, pp.308-312, Doi: 10.1016/j.phpro.2015.09.143.

[12] Aggarwal A.K., Kaura S.K., Chhachhia D.P., Sharma A.K, Kumar R., Interferometry based security hologram readable with an encoded key hologram, Indian Journal of Pure and Applied Physics 42, 2004, pp.816-819.

[13] Keerthy K S, S Ambadiyil, A K Jha and R Prabhu, Speckle Pattern Analysis of Security Holograms and related Foils for Quality Assessment and Authentication, Proceedings Volume 12275, Counterterrorism, Crime Fighting, Forensics, and Surveillance Technologies VI; 1227509 (2022) https://doi.org/10.1117/12.2635446, SPIE Sensors & Imaging, Berlin, 5-7 Sept. 2022.

[14] S Ambadiyil, Sreelekshmi.R.C, V.P.M. Pillai and R. Prabhu, Holographic interferometry for security and forensic applications, SPIE-Security + Defence, Edinburgh, United Kingdom, 26 - 29 September 2016. https://doi.org/10.1117/12.2242153

[15] Lai S., Security holograms using an encoded reference wave, optical Engineering 35(9), 1996, p.2470, DOI: 10.1117/1.600850

[16] Aggarwal A.K., Kaura S.K., Chhachhia D.P., Sharma A.K., Encoded reference wave security holograms with enhanced features, journal of Optics A:Pure and Applied Optics 6(2),2004,p.278, DOI: 10.088/1464-4258/6/2/020.

[17] Liu. S., Zhang X, Lai.H., Artistic effect and application of moire patterns in security holograms, Applied Optics 34(22), 1995, pp.8096-8097, DOI: 10.1364/AO.36.008096.

[18] Ahang X., Dalsgaard E., Liu S., Lai H., Chen J., Concealed holographic coding for security applications by using a moire technique, Applied Optics 36(31), 1997, pp.8096-8097, DOI: 10.1364/AO.36.008096.

[19] Aggarwal A.K., Kaura S.K., Chhachhia D.P., Sharma A.K., Concealed moire pattern encoded security holograms readable by a key hologram, Optics and Laser technology 38(2), 2006, pp.117-121, DOI: 10.1016/j.optlastec.2004.10.010.