様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２８　年　　５　月　１９　日現在

機関番号：　１２１０１
研究種目：　挑戦的萌芽研究
研究期間：　2014～2015
課題番号：　２６５４００５４

研究課題名（和文）レーザースペックルを用いた視覚復号型秘密分散暗号法の開発研究

研究課題名（英文）Developement research into the visual secret sharing (visual cryptography) that uses laser speckles

研究代表者

鵜野　克宏（Uno, Katsuhiro）

茨城大学・工学部・准教授

研究者番号：１０２８０７１０

交付決定額（研究期間全体）：（直接経費）　　3,000,000円

研究成果の概要（和文）：単独では意味を持たないが、合成すると秘密画像が再生される視覚復号型暗号を実現するために、従来のランダムグリッドに替わり、粗面からの散乱光によるスペックルパターンを初めて用いた。秘密画像が埋め込まれたランダムパターンであるシェアを作成するために、スペックルパターンを切り出し、二値化した。このシェアと元のスペックルパターンを重ね合わせることにより、秘密画像を再生することに成功した。これは、直接シェアにスペックルパターンを照射することによって、秘密画像を解読できることを意味する。

研究成果の概要（英文）：We used for the first time the speckle pattern created by the scattered laser beam from rough surfaces in order to perform the visual secret sharing that is cryptography method of hiding a secret image by stacking two meaningless random pattern, which is alternative material for random grid pattern. Segmentation and binarization of the speckle pattern was performed for making one share embedding secret image. Reconstruction of the secret image was successfully achieved by the product between the share and the original speckle pattern. This means that it is able to decode the secret image by irradiating directly the speckle pattern into the share.

研究分野：　光情報処理

キーワード：　視覚復号型秘密分散法　視覚復号型暗号法　スペックル　ランダムグリッド

１．研究開始当初の背景

一つの画像を二つ以上の複数の媒体にランダムに分散し、各々の媒体からは情報を復元することができず、すべての媒体を重ねることによってのみ情報が復元される暗号化法を視覚復号型秘密分散法、または視覚復号型暗号法という。この方法は、復号時に計算機などの処理を必要とせず、記録媒体として紙や OHP フィルムなどが利用できるため、災害時に計算機がダウンした場合に備えた秘密情報の保持に有用な技術である。この技術の問題点は媒体を重ねて復号するため、最下層以外は、OHP フィルムなどの透明な媒体を必要とすること、画像サイズに応じた大きさの媒体が必要となることなどがあげられる。この問題点を解決するために、本研究では、秘密画像を複数の媒体に分散する代わりに、粗面からのレーザー光の散乱光を投影した時に現れるスペックルを鍵として画像を復元する新しい方法を提案し、その実証研究が行われた。この方法により、照明光それ自体が復号媒体となるために、透明な媒体を必要とせず、粗面のごく小さな領域から、復号に必要な十分な大きさのランダム画像を生成することができるため、必ずしも画像と同じ大きさの媒体を必要としない。さらに、粗面のミクロな形状が、鍵となるスペックルの構造を決定するため、復号にスペックルを使用することは、複製が極めて困難である非常にセキュアな暗号化法となり得る。

しかし、復号にスペックルを使用する方法にも、いくつか解決しなければならない問題点がある。その一つは、通常の視覚復号型暗号で用いられるシャアと呼ばれるランダム画像は、白（透明）か黒（不透明）の 2 値画像であるのに対して、スペックルはその間の濃度を連続的にとり得るため、2 値論理で用いられる論理演算が使えないことである。他には、粗面の微視的構造がスペックルの平均強度を変化させてしまうため、平均的な明るさが均一ではない散乱光が得られてしまう点がある。

２．研究の目的

本研究の第一の目的は、粗面からのレーザー光の散乱光によって発生するスペックルパターンを用いて、秘密画像を光の吸収率がランダムに変化するシェアとして暗号化することである。第二の目的は、暗号化されたシェアに、暗号化した時と同じレーザースペックルパターンを照射し、元の秘密画像を復元することである。

３．研究の方法

平成 26 年度は、ランダムでコントラストの高いスペックルパターンを発生させる光学系を構築することを目指した。

図１に示すように、レーザー光源からのコヒーレント光を、レンズ系で任意のスポット径に変換して粗面に照射した。粗面から反射・散乱されたレーザー光をスクリーンに投影し、このときスクリーン上に現れるスペックルパターンを CCD カメラに取り込み、シェアの元になる画像を取得した。当初、粗面とスクリーンは、精密な位置決めを行なうために、自動制御の移動ステージに固定する予定であった。しかし、自動制御プログラムの作成に時間を要することから、手動の XYZ アオリ付ステージを用いた。また、その他の光学系は、振動を除去するために除振台上のレールに固定した。

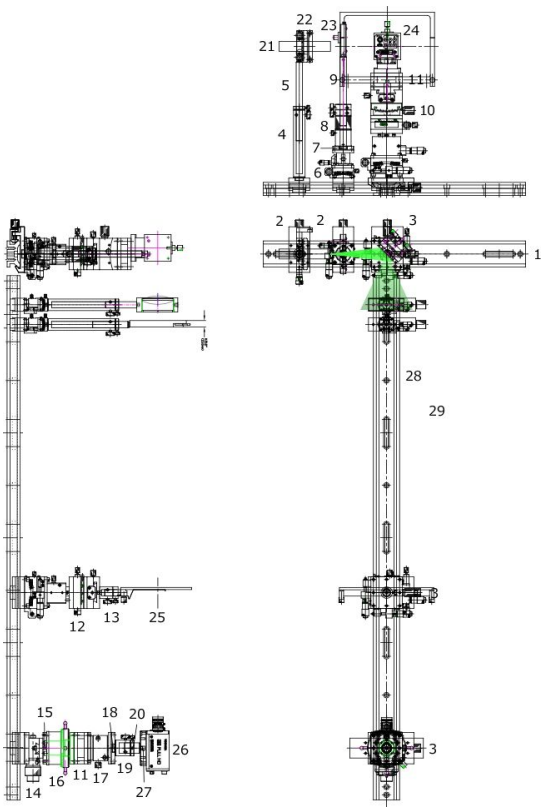

図 1　実験光学系

スペックルパターンのコントラストや平均粒径は、粗面の粗さやレーザー照射スポット径に依存するので、当初、表面粗さを制御した金属板、あるいは擦りガラスを作製し、レンズ系を制御することによりレーザースポット径を調節して、所望のコントラスト、および粒径のスペックルパターンを生成する予定であった。しかし、金属板では圧延痕により、一方向に伸びたスペックル画像しか得られなかった。そこで、十分なコントラストを得るために、照射波長に比べて十分大きな粗さを持つと考えられるコピー用紙と、表面粗さが抑えられた光沢紙を粗面として用いた。また、レンズで照射ビームを集光して、スペックルの平均粒径を適当な大きさに調節した。

また、スペックルパターンを投影するスクリーンに材質の異なる様々な物を用い、それによって取得されるスペックル画像の違いについても調べた。まず、スクリーンに異なる濃淡パターンを印刷し、レーザーを照射して反射光、および透過光の強度を測定した。これは、反射光の濃淡パターンを実際の濃淡パターンに近づけるための補正用の校正曲

線を求める目的で行なった。スクリーンの材質として再生紙と擦りガラスを用いた。印刷方法としてレーザープリンターを用いた。

つぎに、計算機を用いて取得されたスペックル画像に秘密画像を埋め込んだシェアを作成し、画像の秘匿性を検証した。なお、スペックル画像に秘密画像を埋め込む際、前述の論理演算の問題から､両画像を 2 値化した。スペックルの平均粒径やコントラストを調整し、秘密画像が認識できなくなる最適条件を調べた。

平成 27 年度は、スペックル画像に秘密画像を埋め込んだシェアとスペックル画像を重ね合わせ、画像の復号を行った。

まず、カメラに撮り込んだスペックル画像に秘密画像を埋め込んだシェアに、元のスペックル画像を計算機上で重ね合わせ、画像の復号ができるかを確認した。

最後に、レーザー光を粗面に照射し、スペックルを発生させ、それをスクリーンに投影した画像をカメラに取り込んでスペックル画像を作成し、そのスペックル画像を 2 値化した画像に秘密画像を埋め込んだ分散画像をスクリーンの位置に戻し、スペックル画像を取得したときと同じ光学系を用いて、全く同じスペックルパターンを照射し、画像の復号を試みた。

４．研究成果

まず、図 2 の濃淡パターンに対する反射光、および透過光の応答を図 3、および図 4 に示す。図では、直接光を避けるために、下方にずらして撮影した濃淡パターンを示している。この結果、反射光の応答では、濃淡差がほとんど現れないのに対して、透過光ではある程度の差が現れることが分かった。このことから、シェアの照明方法は、反射型よりも透過型が適切であることが分かった。

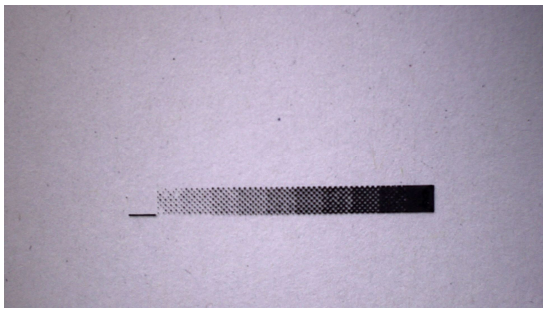

図 2　濃淡パターン

図 3　濃淡パターンの反射光

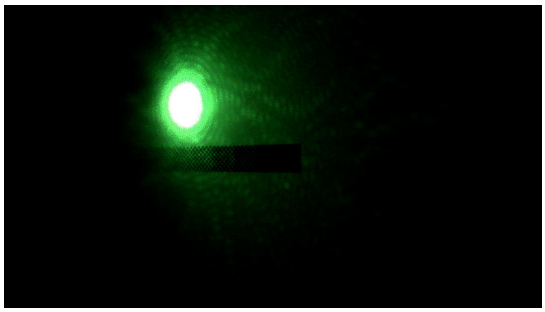

図 4　濃淡パターンの透過光

図 1 の光学系により得られたスペックルパターンを図 5 に示す。粗面として用いられた紙のミクロな構造は、有限な大きさの繊維であるため、得られたスペックルパターンは、中央部が明るく周囲が暗くなり、一様なパターンが得られなかった。そのため、得られたスペックルパターンを CCD カメラに取り込んだのち、中央部の明るい部分のみを切り出して、シェアを作成するためのランダムパターンとした。そのランダムパターンを図 6 に示す。そのパターンと秘密画像とのランダムな置き換えにより、元の画像が推測されないようなランダムで意味のないパターンとしてシェアを作成した。

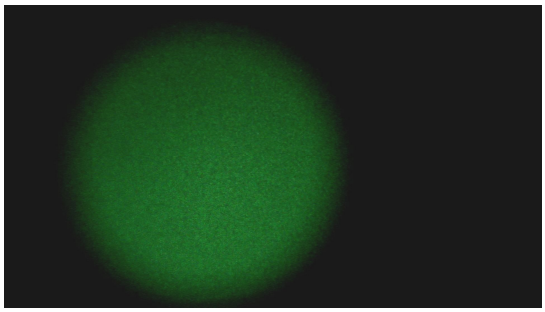

図 5　スペックルパターン

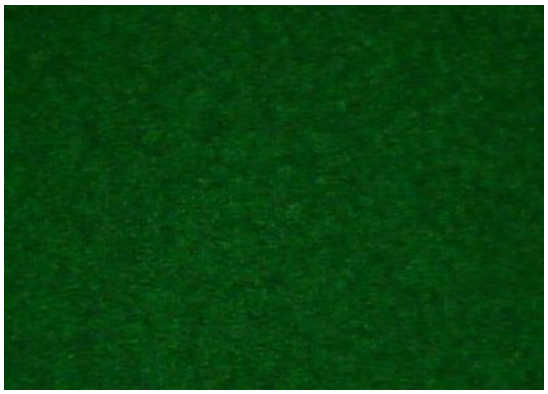

図 6　ランダムパターン

その際、スペックルパターンが連続した輝度分布であるために、秘密画像との単純な置き換えでは秘密画像の特徴が残ってしまい、元の画像が推測されてしまうため、置き換えを行う前に、スペックルパターンと秘密画像を 2 値化した（図 7、図 8）。

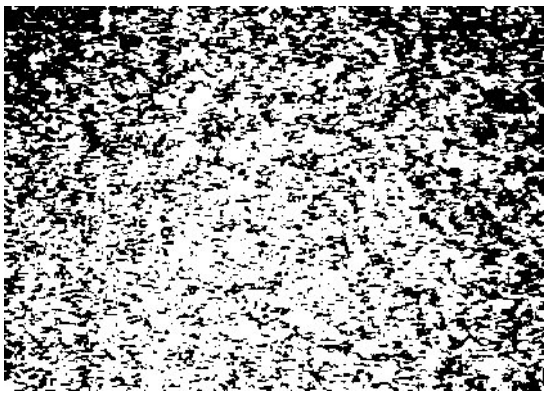

図 7　二値化されたランダムパターン

図 8　二値化された秘密画像

しかし、2 値化したスペックルパターンと秘密画像を置き換えても、画像の中心部分と周辺部分で明るさが異なっているために、部分的に秘密画像の特徴が現れてしまい、完全にランダム化されたシェアが得られなかった（図 9）。これは、散乱体である紙のミクロな構造が有限な大きさであるため、レーザー光の散乱角も有限となり、そのためそれらの干渉として生じるスペックルの平均強度は、散乱角が大きくなるに伴い小さくなることからくる避けられない現象である。この問題に対して、得られたスペックルパターンの画像をいくつかの領域に分割し、それぞれに異なる閾値で 2 値化することにより平均強度の差を解消し、均一なランダムパターン（図 10）を得ることに成功した。この均一化されたランダムパターンにより作成されたシェアを図 11 に示す。

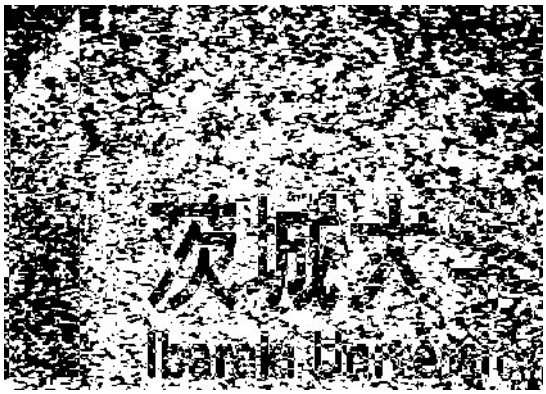

図 9　二値化されたランダムパターンを用いたシェア

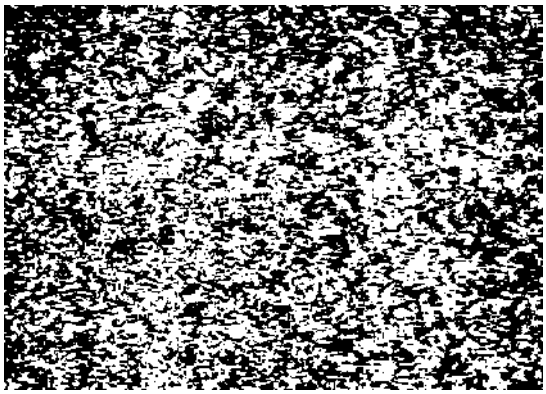

図 10　均一化されたランダムパターン

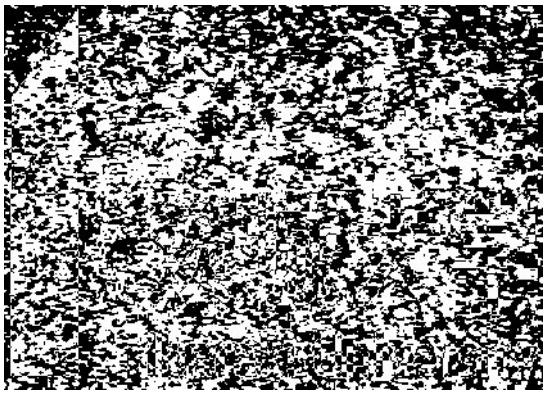

図 11　均一化されたランダムパターンを用いたシェア

第二の目的を実現するために、上記と同様の方法で作成したシェア（図 12）を OHP に記録し、スペックルパターンを投影した摺りガラス上に設置し、シェアを作成した時と同じ散乱光を照射した。そして、シェアを通過した透過光を、シェアに焦点を合わせた CCD カメラで撮影した。シェアを OHP で作成した理由は、上記の濃淡パターンの実験に

よる結果に加えて、透過光を観察する光学系の方が、光軸が一直線となるために、扱いやすいという理由による。もちろん、反射型の光学系に変えればOHPは必要ない。

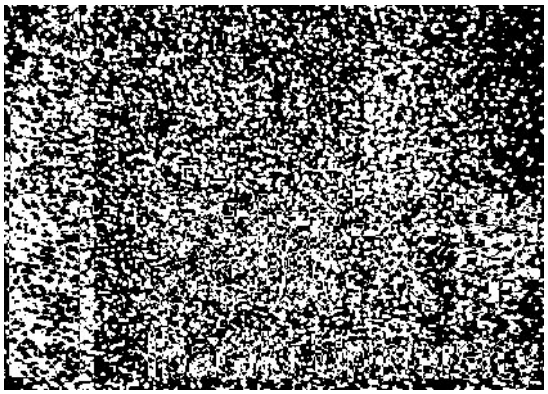

図 12　作成されたシェア

しかし、記録時とまったく同じ散乱光を照射したにもかかわらず、シェアを透過した光をCCDで記録した画像からは、秘密画像を確認することができなかった(図 13)。そこで、レーザー光を直接シェアに照射する前の段階として、スペックルパターンを同じパターンとシェアの積を計算したところ、ノイズとコントラストを調整すると、秘密画像を再生することができた(図 14)。これは、計算機上の積は、画像の強度分布情報のみを用いているのに対して、スペックル照明光には光の振幅に加え、位相の情報も含まれていることに起因していると考えられる。このことから、シェアに照射された散乱光の位相が、再生結果に影響を与えていることが示唆された。

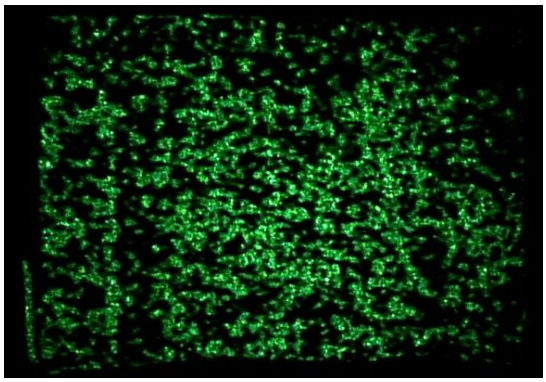

図 13　スペックル照射による再生像

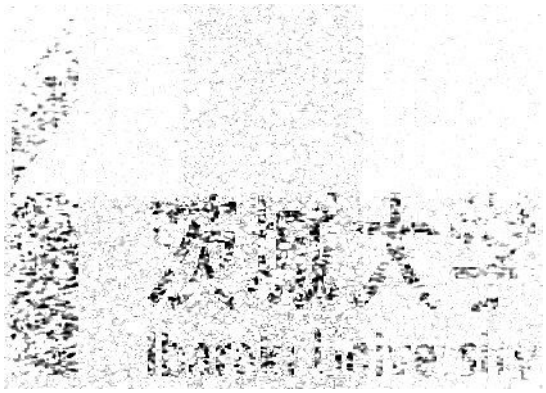

図 14　スペックルパターンとシェアの積による再生像

上記の結果を学術論文としてまとめ、産業応用工学会主催の国際会議、および論文誌（英語）に投稿し、斬新な発想と興味深い結果であり、国内外に例がない研究例として評価された。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　１件）

① Katsuhiro Uno, Hoan Hoa Tien Dung, “Visual Cryptography by Speckle Pattern Illumination”, Journal of the Institute of Industrial Applications Engineers Vol.4, No.1, pp.26-32, (2016.1.25), 査読有
DOI: 10.12792/JIIAE.4.26

〔学会発表〕（計　１件）

① Katsuhiro Uno, Hoang H. T. Dung, “Visual Secret Sharing by Speckle Pattern Illumination”, 3rd IIAE International Conference on Intelligent Systems and Image Processing, 2015.9.03, 福岡大学（福岡県福岡市）

６．研究組織
(1)研究代表者
鵜野　克宏（Katsuhiro Uno）
茨城大学・工学部・准教授

研究者番号：10280710

(2)研究分担者
無し

(3)連携研究者
無し